Glossary

1 gigabit Ethernet — An Ethernet standard for networks that achieve 1-Gbps maximum throughput. 1 Gigabit Ethernet runs (preferably) on fiber, but may also run over twisted pair. It is primarily used for network backbones.

1 gigabit per second (Gbps) — 1,000,000,000 bits per second.

1 kilobit per second (Kbps) — 1000 bits per second.

1 megabit per second (Mbps) — 1,000,000 bits per second.

1 terabit per second (Tbps) — 1,000,000,000 bits per second.

3-tier architecture — A client/server environment that uses middleware to translate requests between the client and server.

10 Gigabit Ethernet — A standard currently being defined by the IEEE 802.3ae committee. 10 Gigabit Ethernet will allow 10-Gbps throughput and will include full-duplexing and multimode fiber requirements.

100BaseFX — A Physical layer standard for networks that specifies baseband transmission, multimode fiber cabling, and 100-Mbps throughput. 100BaseFX networks have a maximum segment length of 400 meters. 100BaseFX may also be called "Fast Ethernet."

100BaseT — A Physical layer standard for networks that specifies baseband transmission, twisted-pair cabling, and 100-Mbps throughput. 100BaseT networks have a maximum segment length of 100 meters and use the star topology. 100BaseT is also known as Fast Ethernet.

100BaseT4 — A type of 100BaseT network that uses all four wire pairs in a twisted-pair cable to achieve its 100-Mbps throughput. 100BaseT4 is not capable of full-duplex transmission and requires CAT3 or higher media.

100BaseTX — A type of 100BaseT network that uses two wire pairs in a twisted-pair cable, but uses faster signaling to achieve 100-Mbps throughput. It is capable of full-duplex transmission and requires CAT5 or higher media.

100BaseVG (100VG-AnyLAN) — A Physical layer standard for networks that specifies baseband transmission, twisted-pair media, and 100-Mbps throughput. 100BaseVG uses a different and more efficient method than 100BaseT for allowing nodes to transmit data on the media. However, 100BaseVG is rarely used.

10Base2 — See *Thinnet*.

10Base5 — See *Thicknet*.

10BaseF — A Physical layer standard for networks that specifies baseband transmission, multimode fiber cabling, and 10-Mbps throughput. 10BaseF networks have a maximum segment length of 1000 or 2000 meters, depending on the version, and employ a star topology.

10BaseT — A Physical layer standard for networks that specifies baseband transmission, twisted pair media, and 10-Mbps throughput. 10BaseT networks have a maximum segment length of 100 meters and rely on a star topology.

802.3 — The IEEE standard for Ethernet networking devices and data handling.

802.3 Raw — See *Novell proprietary 802.3 frame*.

802.4 — The IEEE standard for Token Bus networking devices and data handling.

802.5 — The IEEE standard for Token Ring networking devices and data handling.

802.6 — The IEEE standard for Metropolitan Area Network (MAN) networking.

802.10 — The IEEE standard that describes network access controls, encryption, certification, and other security topics.

802.11 — The IEEE standard for wireless networking.

A+ — Professional certification established by CompTIA that verifies knowledge about PC operation, repair, and management.

access method — A network's method of controlling how network nodes access the communications channel. CSMA/CD is the access method used by Ethernet networks.

access server — See *communications server*.

account — A record of a user that contains all of his or her properties, including rights to resources, password, username, and so on.

acknowledgment (ACK) — A response generated at the Transport layer of the OSI Model that confirms to a sender that its frame was received.

Active Directory — Windows 2000 Server's method for organizing and managing objects associated with the network.

active monitor — On a Token Ring network, the workstation that maintains timing for token passing, monitors token and frame transmission, detects lost tokens, and corrects problems when a timing error or other disruption occurs. Only one workstation on the ring can act as the active monitor at any given time.

active topology — A topology in which each workstation participates in transmitting data over the network.

adapter card — See *expansion board*.

address — A number that uniquely identifies each workstation and device on a network. Without unique addresses, computers on the network could not reliably communicate.

address management — Centrally administering a finite number of network addresses for an entire LAN. Usually this task can be accomplished without touching the client workstations.

Address Resolution Protocol (ARP) — A core protocol in the TCP/IP suite that belongs in the Internet layer. It obtains the MAC (physical) address of a host, or node, and then creates a local database that maps the MAC address to the host's IP (logical) address.

address resource record — A type of DNS data record that maps the IP address of an Internet-connected device to its domain name.

addressing — The scheme for assigning a unique identifying number to every workstation and device on the network. The type of addressing used on a network depends on its protocols and network operating system.

Administrator — A user account that has unlimited privileges to resources and objects managed by a server or domain. The administrator account is created during NOS installation.

AIX — IBM's proprietary implementation of the UNIX system.

alias — A nickname for a node's host name. Aliases can be specified in a local host file.

alien crosstalk — A type of interference that occurs when signals from an adjacent cable interfere with another cable's transmission.

amplifier — A device that boosts, or strengthens, an analog signal.

amplitude — A measure of a signal's strength.

amplitude modulation (AM) — A modulation technique in which the amplitude of the carrier signal is modified by the application of a data signal.

analog — A signal that uses variable voltage to create continuous waves, resulting in an inexact transmission.

ANSI (American National Standards Institute) — An organization composed of more than 1000 representatives from industry and government who together determine standards for the electronics industry in addition to other fields, such as chemical and nuclear engineering, health and safety, and construction.

anycast address — A type of address specified in IPv6 that represents a group of interfaces, any one of which (and usually the first available of which) can accept a transmission. At this time, anycast addresses are not designed to be assigned to hosts, such as servers or workstations, but rather to routers.

Apache — A popular open source software Web server application often used on Linux Internet servers.

AppleTalk — The protocol suite used to interconnect Macintosh computers. Although AppleTalk was originally designed to support peer-to-peer networking among Macintoshes, it can now be routed between network segments and integrated with NetWare- or Microsoft-based networks.

AppleTalk network number — A unique 16-bit number that identifies the network to which an AppleTalk node is connected.

AppleTalk node ID — A unique 8-bit or 16-bit (if you are using extended networking, in which a network can have multiple addresses and support multiple zones) number that identifies a computer on an AppleTalk network.

AppleTalk zone — Logical groups of computers defined on an AppleTalk network.

Application layer — The seventh layer of the OSI Model. The Application layer provides interfaces to the software that enable programs to use network services.

application programming interface (API) — A routine (or set of instructions) that allows a program to interact with the operating system. APIs belong to the Application layer of the OSI Model.

application switch — Another term for a Layer 3 or Layer 4 switch.

ARP table — The database that lists MAC addresses and their associated IP addresses used for ARP queries.

array — A group of hard disks.

asset management — A system for collecting and storing data on the quantity and types of software and hardware assets in an organization's network.

asymmetric encryption — A type of encryption (such as public key encryption) that uses a different key for encoding data than is used for decoding the cipher text.

asymmetric multiprocessing — A multiprocessing method that assigns each subtask to a specific processor.

asymmetrical — The characteristic of a transmission technology that affords greater bandwidth in one direction (either from the customer to the carrier, or vice versa) than in the other direction.

asymmetrical DSL — A variation of DSL that offers more throughput when data travels downstream—downloading from a local carrier's POP to the customer—than when it travels upstream—uploading from the customer to the local carrier's POP.

asynchronous — A transmission method in which data being transmitted and received by nodes do not have to conform to any timing scheme. In asynchronous communications, a node can transmit at any time and the destination node must accept the transmission as it comes.

Asynchronous Transfer Mode (ATM) — A technology originally conceived in 1983 at Bell Labs, but standardized only in the mid-1990s. It relies on a fixed packet size to achieve data transfer rates up to 9953 Mbps. The fixed packet consists of 48 bytes of data plus a 5-byte header. The fixed packet size allows ATM to provide predictable traffic patterns and better control over bandwidth utilization.

attenuate — To lose signal strength as a transmission travels farther away from its source.

attenuation — A signal's loss of strength as it travels farther from its source.

attribute — A variable property associated with a network object. For example, a restriction on the time of day a user can log on is an attribute associated with that user object.

AUI (Attachment Unit Interface) — An Ethernet standard for connecting coaxial cables with transceivers and networked nodes.

authentication — The process whereby a network operating system verifies that a client's user name and password are valid and allows the client to log onto the network.

authentication header (AH) — In the context of IPSec, a type of encryption that provides authentication of the IP packet's data payload through public key techniques.

authentication service (AS) — In Kerberos terminology, the process that runs on a key distribution center (KDC) to initially validate a client who's logging in. The authentication service issues session keys to the client and the service the client wants to access.

authenticator — In Kerberos authentication, the user's timestamp encrypted with the session key. The authenticator is used to help the service verify that a user's ticket is valid.

autosense — A feature of modern NICs that enables a NIC to automatically sense what types of frames are running on a network and set itself to that specification.

availability — How consistently and reliably a file, device, or connection can be accessed by authorized personnel.

B channel — In ISDN, the "bearer" channel, so named because it bears traffic from point to point.

backbone — The cabling or part of a network that connects separate LAN segments. Backbone wiring provides interconnection between telecommunications closets, equipment rooms, and entrance facilities.

backleveling — The process of reverting to a previous version of a software program after attempting to upgrade it.

back up — A copy of data or program files created for archiving or safekeeping purposes.

backup — The process of copying critical data files to a secure storage area. Often backups are performed according to a formulaic schedule.

backup rotation scheme — A plan for when and how often backups occur, and which backups are full, incremental, or differential.

bandwidth — A measure of the difference between the highest and lowest frequencies that a medium can transmit.

bandwidth overhead — The burden placed on the underlying network to support a routing protocol.

base I/O port — A setting that specifies, in hexadecimal notation, which area of memory will act as a channel for moving data between the network adapter and the CPU. Like its IRQ, a device's base I/O port cannot be used by any other device.

baseband — A form of transmission in which digital signals are sent through direct current pulses applied to the wire. This direct current requires exclusive use of the wire's capacity, so baseband systems can transmit only one signal, or one channel, at a time. Every device on a baseband system shares a single channel.

baseline—A record of how well the network operates under normal conditions (including its performance, collision rate, utilization rate, and so on). Baselines are used for comparison when conditions change.

baselining — The practice of measuring and recording a network's current state of operation.

bend radius — The radius of the maximum arc into which you can loop a cable before you will cause data transmission errors. Generally, a twisted-pair cable's bend radius is equal to or greater than four times the diameter of the cable.

best path — The most efficient route from one node on a network to another. Under optimal network conditions, the best path is the most direct path between two points.

binary — A system founded on using 1s and 0s to encode information.

binding — The process of assigning one network component to work with another.

bio-recognition access — A method of authentication in which a device scans an individual's unique physical characteristics (such as the color patterns in his or her eye's iris or the geometry of his or her hand) to verify the user's identity.

BIOS (basic input/output system) — Firmware attached to the system board that controls the computer's communication with its devices, among other things.

bit — Short for binary digit. A bit equals a single pulse in the digital encoding system. It may have only one of two values: 0 or 1.

blackout — A complete power loss.

block — A unit of disk space and the smallest unit of disk space that can be controlled by the NetWare system. Smaller blocks require more server memory.

block ID — The first set of six characters that make up the MAC address and that are unique to a particular vendor.

block suballocation — A NetWare technique for using hard disk space more efficiently. Files that don't fit neatly into a whole number of blocks can take up fractions of blocks, leaving the remaining fractions free for use by other data.

BNC barrel connector — A connector used on Thinnet networks with two open ends used to connect two Thinnet coaxial cables.

BNC T-connector — A connector used on Thinnet networks with three open ends. It attaches to the Ethernet interface card at the base of the "T" and to the Thinnet cable at its two sides so as to allow the signal in and out of the NIC.

bonding — The process of combining more than one bearer channel of an ISDN line to increase throughput. For example, BRI's two 64-Kbps B channels are bonded to create an effective throughput of 128 Kbps.

boot sector virus — A virus that resides on the boot sector of a floppy disk and is transferred to the partition sector or the DOS boot sector on a hard disk. A boot sector virus can move from a floppy to a hard disk only if the floppy disk is left in the drive when the machine starts up.

Bootstrap Protocol (BOOTP) — A service that simplifies IP address management. BOOTP maintains a central list of IP addresses and their associated devices' MAC addresses, and assigns IP addresses to clients when they request it.

Border Gateway Protocol (BGP) — The routing protocol of Internet backbones. The router stress created by Internet growth has driven the development of BGP, the most complex of the routing protocols. The developers of BGP had to contend with the prospect of 100,000 routes as well as the goal of routing traffic efficiently and fairly through the hundreds of Internet backbones.

braiding — A braided metal shielding used to insulate some types of coaxial cable.

BRI (Basic Rate Interface) — A variety of ISDN that uses two 64-Kbps bearer channels and one 16-Kbps data channel, as summarized by the following notation: 2B + D. BRI is the most common form of ISDN employed by home users.

bridge — A device that looks like a repeater, in that it has a single input and a single output, but is different from a repeater in that it can interpret the data it retransmits.

bridge router (brouter) — A router capable of providing Layer 2 bridging functions.

broadband — 1) A form of transmission in which signals are modulated as radiofrequency analog pulses with different frequency ranges. Unlike baseband, broadband technology does not involve binary encoding. The use of multiple frequencies enables a broadband system to operate over several channels and therefore carry much more data than a baseband system. 2) A group of network connection types or transmission technologies that are generally capable of exceeding 1.544 Mbps throughput. Examples of broadband include DSL and SONET.

broadcast — A transmission that involves one transmitter and multiple receivers.

broadcast domain — In a virtual local area network (VLAN), a combination of ports that make up a Layer 2 segment and must be connected by a Layer 3 device, such as a router or Layer 3 switch.

brouter — See *bridge router*.

brownout — A momentary decrease in voltage, also known as a *sag*. An overtaxed electrical system may cause brownouts, recognizable as a dimming of the lights.

browser — Software that provides clients with a simple, graphical interface to the Web.

BSD (Berkeley Software Distribution) — A UNIX distribution that originated at the University of California at Berkeley. The BSD suffix differentiates these distributions from AT&T distributions. No longer being developed at Berkeley, the last public release of BSD UNIX was version 4.4.

bug — A flaw in software or hardware that causes it to malfunction.

bus — 1) The single cable connecting all devices in a bus topology. 2) The type of circuit used by the system board to transmit data to components. Most new Pentium computers use buses capable of exchanging 32 or 64 bits of data. As the number of bits of data a bus handles increases, so too does the speed of the device attached to the bus.

bus topology — A topology in which a single cable connects all nodes on a network without intervening connectivity devices.

byte — Eight bits of information. In a digital signaling system, broadly speaking, one byte carries one piece of information.

cable checker — A simple handheld device that determines whether cabling can provide connectivity. To accomplish this task, a cable checker applies a small voltage to each conductor at one end of the cable, then checks whether that voltage is detectable at the other end. It may also verify that voltage cannot be detected on other conductors in the cable.

cable drop — Fiber-optic or coaxial cable that connects a neighborhood cable node to a customer's house.

cable modem — A device that modulates and demodulates signals for transmission and reception via cable wiring.

cable plant — The hardware that constitutes the enterprise-wide cabling system.

cable tester — A handheld device that not only checks for cable continuity, but also ensures that the cable length is not excessive, measures the distance to a cable fault, measures attenuation along a cable, measures near-end crosstalk between wires, measures termination resistance and impedance for Thinnet cabling, issues pass/fail ratings for wiring standards, and stores and prints cable testing results.

caching — The process of saving frequently used data to an area of the physical memory so that it becomes more readily available for future requests. Caching accelerates the process of accessing the server because the operating system no longer needs to search for the requested data on the disk.

call tracking system — A software program used to document problems (also known as help desk software). Examples of popular call tracking systems include Clientele, Expert Advisor, Professional Help Desk, Remedy, and Vantive.

capacity — See *throughput.*

Carrier Sense Multiple Access/Collision Avoidance (CSMA/CA) — A network access method used on LocalTalk networks in which nodes on a shared communication channel signal their intent to transmit data before doing so, thus avoiding collisions.

Carrier Sense Multiple Access/Collision Detection (CSMA/CD) — Rules for communication used by shared Ethernet networks. In CSMA/CD each node waits its turn before transmitting data, to avoid interfering with other nodes' transmissions.

CAT — Abbreviation for the word "category" when describing a type of twisted-pair cable. For example, Category 3 unsheilded twisted-pair cable may also be called CAT3. See *Category 1, Category 2, Category 3, Category 4, Category 5, Enhanced Category 5, Category 6,* and *Category 7.*

Category 1 (CAT1) — A form of UTP that contains two wire pairs. CAT1 is suitable for voice communications, but not for data. At most, it can carry only 20 Kbps of data.

Category 2 (CAT2) — A form of UTP that contains four wire pairs and can carry up to 4 Mbps of data. CAT2 is rarely found on modern networks, because most require higher throughput.

Category 3 (CAT3) — A form of UTP that contains four wire pairs and can carry up to 10-Mbps, with a possible bandwidth of 16 MHz. CAT3 has typically been used for 10-Mbps Ethernet or 4-Mbps Token Ring networks. Network administrators are gradually replacing CAT3 cabling with CAT5 to accommodate higher throughput. CAT3 is less expensive than CAT5.

Category 4 (CAT4) — A form of UTP that contains four wire pairs and can support up to 16-Mbps throughput. CAT4 may be used for 16-Mbps Token Ring or 10-Mbps Ethernet networks. It is guaranteed for data transmission up to 20 MHz and provides more protection against crosstalk and attenuation than CAT1, CAT2, or CAT3.

Category 5 (CAT5) — The most popular form of UTP for new network installations and upgrades to Fast Ethernet. CAT5 contains four wire pairs and supports up to 100-Mbps throughput and a 100 MHz signal rate. In addition to 100-Mbps Ethernet, CAT5 wiring can support other fast networking technologies, such as Asynchronous Transfer Mode (ATM) and Fiber Distributed Data Interface (FDDI).

Category 5 enhanced (CAT5e) — See *enhanced Category 5.*

Category 6 (CAT6) — A twisted-pair cable that contains four wire pairs, each wrapped in foil insulation. Additional foil insulation covers the bundle of wire pairs, and a fire-resistant plastic sheath covers the second foil layer. The foil insulation provides excellent resistance to crosstalk and enables CAT6 to support at least six times the throughput supported by regular CAT5.

Category 7 (CAT7) — A twisted-pair cable that contains multiple wire pairs, each separately shielded then surrounded by another layer of shielding within the jacket. CAT7 can support up to a 1-GHz signal rate. But because of its extra layers, it is less flexible than other forms of twisted-pair wiring.

CD-ROM File System (CDFS) — The read-only file system used to access resources on a CD. Windows 2000 supports this file system to allow CD-ROM file sharing.

cell — A packet of a fixed size. In ATM technology, a cell consists of 48 bytes of data plus a 5-byte header.

certification — The process of mastering material pertaining to a particular hardware system, operating system, programming language, or other software program, then proving your mastery by passing a series of exams.

Certified NetWare Engineer (CNE) — Professional certification established by Novell that demonstrates an in-depth understanding of Novell's networking software, including NetWare.

change management system — A process or program that provides support personnel with a centralized means of documenting changes made to the network. In smaller organizations, a change management system may be as simple as one document on the network to which networking personnel continually add entries to mark their changes. In larger organizations, it may consist of a database package complete with graphical interfaces and customizable fields tailored to the particular computing environment.

channel — A distinct communication path between two or more nodes, much like a lane is a distinct transportation path on a freeway. Channels may be separated either logically (as in multiplexing) or physically (as when they are carried by separate wires).

child domain — A domain found beneath another domain in a Windows 2000 domain tree.

cipher text — The unique data block that results when an original piece of data (such as text) is encrypted (for example, by using a key).

CIR (committed information rate) — The guaranteed minimum amount of bandwidth selected when leasing a frame relay circuit. Frame relay costs are partially based on CIR.

circuit switching — A type of switching in which a connection is established between two network nodes before they begin transmitting data. Bandwidth is dedicated to this connection and remains available until users terminate the communication between the two nodes.

cladding — The glass shield around the fiber core of a fiber-optic cable. Cladding acts as a mirror, reflecting light back to the core in patterns that vary depending on the transmission mode. This reflection allows fiber to bend around corners without impairing the light-based signal.

class — A type of object recognized by an NOS directory and defined in an NOS schema. Printers and users are examples of object classes.

client — A computer on the network that requests resources or services from another computer on a network. In some cases, a client could also act as a server. The term "client" may also refer to the user of a client workstation.

Client Services for NetWare (CSNW) — A Microsoft program that can be installed on Windows 2000 clients to enable them to access NetWare servers and make full use of the NetWare Directory System (NDS), its objects, files, directories, and permissions.

client/server architecture — The model of networking in which clients (typically desktop PCs) use a central server to share data, data storage space, and devices.

client/server network — A network based on the client/server architecture.

client_hello — In the context of SSL encryption, a message issued from the client to the server that contains information about what level of security the client's browser is capable of accepting and what type of encryption the client's browser can decipher (for example, RSA or Diffie-Hellman). The client_hello message also establishes a randomly generated number that uniquely identifies the client plus another number that identifies the SSL session.

clustering — See *server clustering*.

CMOS (complementary metal oxide semiconductor) — Firmware on a PC's system board that enables you to change its devices' configurations.

coaxial cable — A type of cable that consists of a central copper core surrounded by an insulator, a braided metal shielding, called braiding, and an outer cover, called the sheath or jacket. Coaxial cable, called "coax" for short, was the foundation for Ethernet networks in the 1980s and remained a popular transmission medium for many years.

collapsed backbone — A type of enterprise-wide backbone in which a router or switch acts as the single central connection point for multiple subnetworks.

collision — In Ethernet networks, the interference of one network node's data transmission with another network node's data transmission.

collision domain — A portion of a LAN encompassing devices that may cause and detect data collisions during transmission. Bridges and switches can logically define the boundaries of a collision domain.

command interpreter — A (usually text-based) program that accepts and executes system programs and applications on behalf of users. Often it includes the ability to execute a series of instructions that are stored in a file.

communications server — A server that runs communications services such as Windows NT's RAS or NetWare's NAS, also known as an access server or remote access server.

CompTIA — See *Computing Technology Industry Association*.

Computing Technology Industry Association (CompTIA) — An association of computer resellers, manufacturers, and training companies that sets industry-wide standards for computer professionals. CompTIA established and sponsors the A+ and Network+ (Net+) certifications.

conduit — Pipeline used to contain and protect the cabling. Conduit is usually made from metal.

connection-oriented — A feature of some protocols that requires the establishment of a connection between communicating nodes before the protocol will transmit data.

connectionless — A feature of some protocols that allows the protocol to service a request without requiring a verified session and without guaranteeing delivery of data.

connectors — The pieces of hardware that connect the wire to the network device, be it a file server, workstation, switch, or printer.

container — A logical receptacle for holding like objects in an NOS directory. Containers form the branches of the directory tree.

container objects — See *container*.

context — A kind of road map for finding an object in an NDS tree. A context is made up of an object's organizational unit names, arranged from most specific to most general, plus the organization name. Periods separate the organizational unit names in context.

contingency planning — The process of identifying steps that will minimize the risk of unforeseen circumstances endangering the quality or timeliness of the project's goals.

Controlled Access Unit (CAU) — A connectivity device used on a Token Ring network. In addition to passing data between nodes, a CAU provides more flexibility and easier management of connected nodes than a MAU.

convergence — The use of networks to carry data, plus video and voice signals.

convergence time — The time it takes for a router to recognize a best path in the event of a change or network outage.

core — The central component of a fiber-optic cable, consisting of one or several pure glass fibers.

core gateways — Gateways that make up the Internet backbone. The Internet Network Operations Center (INOC) operates core gateways.

cracker — A person who uses his or her knowledge of operating systems and utilities to intentionally damage or destroy data or systems.

crossover cable — A twisted-pair patch cable in which the termination locations of the transmit and receive wires on one end of the cable are reversed.

crosstalk — A type of interference caused by signals traveling on nearby wire pairs infringing on another pair's signal.

CSU (channel service unit) — A device used with T-carrier technology that provides termination for the digital signal and ensures connection integrity through error correction and line monitoring.

CSU/DSU — A combination of a CSU (channel service unit) and a DSU (data service unit) that serves as the connection point for a T1 line at the customer's site.

cut-through mode — A switching mode in which a switch reads a frame's header and decides where to forward the data before it receives the entire packet. Cut-through mode is faster, but less accurate, than the other switching method, store and forward mode.

Cyclic Redundancy Check (CRC) — An algorithm used to verify the accuracy of data contained in a data frame.

D channel — In ISDN, the "data" channel used to carry information about the call, such as session initiation and termination signals, caller identity, call forwarding, and conference calling signals.

daisy chain — A linked series of devices.

data encryption standard (DES) — A popular private key encryption technique that was developed by IBM in the 1970s.

Data Link layer — The second layer in the OSI Model. The Data Link layer bridges the networking media with the Network layer. Its primary function is to divide the data it receives from the Network layer into frames that can then be transmitted by the Physical layer.

Data Link layer address — See *MAC address*.

data packet — A discreet unit of information sent from one computer on a network to another.

data propagation delay — The length of time data take to travel from one point on the segment to another point. On Ethernet networks, CSMA/CD's collision detection routine cannot operate accurately if the data propagation delay is too long.

daughter board — See *expansion board*.

daughter card — See *expansion board*.

DB-15 — A general term for connectors that use 15 metal pins to complete a connection between devices. "DB" stands for Data bus, while the number "15" indicates how many pins are used to make the connection.

DB-9 connector — A connector containing nine pins that is used on STP-based Token Ring networks.

dedicated circuit — A continuously available link between two access points that is leased from a communications provider, such as an ISP or telephone company.

default gateway — The gateway that first interprets a device's outbound requests, and then interprets its inbound requests to and from other subnets. In the postal service analogy, the default gateway is similar to a local post office.

demand priority — A method for data transmission used by 100BaseVG Ethernet networks. Each device on a star or hierarchical network sends a request to transmit to the central hub, which grants the requests one at a time. The hub examines incoming data packets, determines the destination node, and forwards the packets to that destination. Because demand priority runs on a star topology, no workstations except the source and destination can "see" the data. Data travel from one device to the hub, then to another device.

demultiplexer (demux) — A device that separates multiplexed signals once they are received and regenerates them in their original form.

denial-of-service attack — A security attack caused by a deluge of traffic that disables the victimized system.

device driver — Software that enables an attached device to communicate with the computer's operating system.

device ID — The second set of six characters that make up a network device's MAC address. The Device ID, which is added at the factory, is based on the device's model and manufacture date.

dial-up — A type of connection that uses modems at the transmitting and receiving ends and PSTN or other lines to access a network.

dial-up networking — The process of dialing into a LAN's access server or into an ISP. Dial-up Networking is also the name of the utility that Microsoft provides with its operating systems to achieve this type of connectivity.

differential backup — A backup method in which only data that have changed since the last backup are copied to a storage medium, and that information is marked for subsequent backup, regardless of whether it has changed.

digital — As opposed to analog signals, digital signals are composed of pulses that can have a value of only 1 or 0.

digital certificate — A password-protected and encrypted file that holds an individual's identification information, including a public key and a private key. The individual's public key is used to verify the sender's digital signature, and the private key allows the individual to log onto a third-party authority who administers digital certificates.

DIP (dual inline package) switch — A small plastic toggle switch on a circuit board that can be flipped to indicate either an "on" or "off" status, which translates into a parameter setting.

direct infrared transmission — A type of infrared transmission that depends on the transmitter and receiver being within the line of sight of each other.

directory — In general, a listing that organizes resources and correlates them with their properties. In the context of network operating systems, a method for organizing and managing objects.

Directory Services Migration Tool (DSMIGRATE) — A tool provided withWindows 2000 Server that enables network administrators to migrate accounts, files, and permissions from a NetWare NDS directory to theWindows 2000 Active Server Directory.

disaster recovery — The process of restoring critical functionality and data to a network after an enterprise-wide outage that affects more than a single system or a limited group of users.

disk mirroring — A RAID technique in which data from one disk are automatically copied to another disk as the information is written.

disk striping — A simple implementation of RAID in which data are written in 64 KB blocks equally across all disks in the array.

diskless workstations — Workstations that do not contain hard disks, but instead rely on a small amount of read-only memory to connect to a network and to pick up their system files.

distinguished name (DN) — A long form of an object's name in Active Directory that explicitly indicates the object name, plus the names of its containers and domains. A distinguished name includes a domain component (DC), organizational unit (OU), and common name (CN). A client uses the distinguished name to access a particular object, such as a printer.

distributed backbone — A type of enterprise-wide backbone that consists of a number of hubs connected to a series of central hubs or routers in a hierarchy.

DIX (Digital, Intel, and Xerox) — A type of AUI connector used on Thicknet networks.

domain — (1) A group of networked devices that share a symbolic name according to Internet standards. For example, workstations used in the Whitehouse share the whitehouse.gov domain name. (2) In the context of Windows NT and Windows 2000 networking, a group of users, servers, and other resources that share account and security policies.

domain account — A type of user account on a Windows 2000 network that has privileges to resources across the domain onto which it is logged.

domain controller — A Windows 2000 server that contains a replica of the Active Directory database.

domain local group — A group on a Windows 2000 network that allows members of one domain to access resources within that domain only.

domain name — The symbolic name that identifies a domain and identifies a group of network nodes. Usually, a domain name is associated with a company or other type of organization, such as a university or military unit.

Domain Name System (DNS) — A hierarchical way of tracking domain names and their addresses, devised in the mid-1980s. The DNS database does not rely on one file or even one server, but rather is distributed over several key computers across the Internet to prevent catastrophic failure if one or a few computers go down. DNS is a TCP/IP service that belongs to the Application layer of the OSI Model.

domain tree — A group of hierarchically arranged domains that share a common namespace in the Windows 2000 Active Directory.

doskey — A command used on MS-DOS and Windows systems that enables the user to recall (using the keyboard's arrow keys) and edit previously entered commands.

dotted decimal notation — The shorthand convention used to represent IP addresses and make them more easily readable by humans. In dotted decimal notation, a decimal number between 1 and 254 represents each binary octet. A period, or dot, separates each decimal.

downstream — A term used to describe data traffic that flows from a local carrier's POP to the customer. In asymmetrical communications, downstream throughput is usually much higher than upstream throughput. In symmetrical communications, downstream and upstream throughputs are equal.

drop cable — The cable that connects a device's Ethernet interface to a transceiver in a Thicknet network.

DS0 (digital signal, level 0) — The equivalent of one data or voice channel in T-carrier technology, as defined by ANSI physical layer standards. All other signal levels are multiples of DS0.

DSL (digital subscriber line) — A dedicated remote connectivity or WAN technology that uses advanced data modulation techniques to achieve extraordinary throughput over regular phone lines. DSL currently comes in seven different varieties, the most common of which is Asymmetric DSL (ADSL).

DSL access multiplexer (DSLAM) — A connectivity device located at a carrier's office that aggregates multiple DSL subscriber lines and connects them to a larger carrier or to the Internet backbone.

DSL modem — A device that demodulates an incoming DSL signal, extracting the information and passing it on to the data equipment (such as telephones and computers) and modulates an outgoing DSL signal.

DSU (data service unit) — A device used in T-carrier technology that converts the digital signal used by bridges, routers, and multiplexers into the digital signal used on cabling. Typically, a DSU is combined with a CSU in a single box, a CSU/DSU.

duplex — See *full-duplex*.

dynamic IP address — An IP address that is assigned to a device through DHCP and may change when the DHCP lease expires or is terminated.

dynamic ARP table entry — A record (of an IP address and its associated MAC address) created in an ARP table when a client makes an ARP request that cannot be satisfied by data already in the ARP table.

Dynamic Host Configuration Protocol (DHCP) — An application layer protocol in the TCP/IP suite that manages the dynamic distribution of IP addresses on a network. Using DHCP to assign IP addresses reduces the effort required to assign addresses and helps prevent duplicate-addressing problems.

dynamic routing — A method of routing that automatically calculates the best path between two nodes and accumulates this information in a routing table. If congestion or failures affect the network, a router using dynamic routing can detect the problems and reroute data through a different path. Most modern networks primarily use dynamic routing.

e-commerce — A means of conducting business over the Web — be it in retailing, banking, stock trading, consulting, or training. Any buying and selling of products or services that occurs over the Internet belongs in the e-commerce category.

echo reply — The response signal sent by a device after another device pings it.

echo request — The request for a response generated when one device pings another device on the network.

EIA (Electronic Industries Alliance) — A trade organization composed of representatives from electronics manufacturing firms across the United States.

electrically erasable programmable read-only memory (EEPROM) — A type of ROM that is found on a circuit board and whose configuration information can be erased and rewritten through electrical pulses.

electromagnetic interference (EMI) — A type of interference that may be caused by motors, power lines, televisions, copiers, fluorescent lights, or other sources of electrical activity.

encapsulation security payload (ESP) — In the context of IPSec, a type of encryption that provides authentication of the IP packet's data payload through public key techniques. In addition, ESP also encrypts the entire IP packet for added security.

encrypted virus — A virus that is encrypted to prevent detection.

encryption — The use of an algorithm to scramble data into a format that can be read only by reversing the algorithm—decrypting the data—to keep the information private. The most popular kind of encryption algorithm weaves a key into the original data's bits, sometimes several times in different sequences, to generate a unique data block.

enhanced CAT5 (CAT5e) — A higher-grade version of CAT5 wiring that contains high-quality copper, offers a high twist ratio, and uses advanced methods for reducing crosstalk. Enhanced CAT5 can support a signaling rate of up to 200 MHz, double the capability of regular CAT5.

Enhanced Interior Gateway Routing Protocol (EIGRP) — A routing protocol developed in the mid-1980s by Cisco Systems that has a fast convergence time and a low network overhead, but is easier to configure and less CPU-intensive than OSPF. EIGRP also offers the benefits of supporting multiple protocols and limiting unnecessary network traffic between routers.

enterprise — An entire organization, including local and remote offices, a mixture of computer systems, and a number of departments. Enterprise-wide computing takes into account the breadth and diversity of a large organization's computer needs.

enterprise-wide network — A network that spans an entire organization and often services the needs of many diverse users. It may include many locations (as a WAN), or it may be confined to one location but include many different departments, floors, and network segments.

Ethernet — A networking technology originally developed at Xerox in 1970 and improved by Digital Equipment Corporation, Intel, and Xerox. Today, four types of Ethernet technology are used on LANs, with each type being governed by a set of IEEE standards.

Ethernet 802.2 frame — See *IEEE 802.3 frame*.

Ethernet 802.3 frame — See *Novell proprietary 802.3 frame*.

Ethernet II frame — The original Ethernet frame type developed by Digital, Intel, and Xerox, before the IEEE began to standardize Ethernet. Ethernet II lacks Logical Link Control layer information but contains a 2-byte type field to identify the upper-layer protocol contained in the frame. It supports TCP/IP, AppleTalk, IPX/SPX, and other higher layer protocols.

expansion board — A circuit board used to connect a device to a computer's system board.

expansion card — See *expansion board*.

expansion slots — Openings on a computer's system board that contain multiple electrical contacts into which the expansion board can be inserted.

explicit one-way trust — A type of trust relationship in which two domains that belong to different NOS directory trees are configured to trust each other.

extended attributes — Attributes beyond the basic Read, Write, System Hidden, and Archive attrevutes supported by FAT.HPFS supports extended attributes.

Extended Industry Standard Architecture (EISA) — A 32-bit bus that is compatible with older ISA devices (because it shares the same length and pin configuration as the ISA bus), but that uses an extra layer of pins (resulting in a deeper, two-layered slot connector) for a second 16 bits to achieve faster throughput. The EISA bus was introduced in the late 1980s to compete with IBM's MCA bus.

extended network prefix — The combination of an address's network and subnet information. By interpreting an address's extended network prefix, a device can determine the subnet to which an address belongs.

external network number — Another term for the network address portion of an IPX/SPX address.

fail-over — The capability for one component (such as a NIC or server) to assume another component's responsibilities without manual intervention.

failure — A deviation from a specified level of system performance for a given period of time. A failure occurs when something doesn't work as promised or as planned.

Fast Ethernet — A type of Ethernet network that is capable of 100-Mbps throughput. 100BaseT and 100BaseFX are both examples of Fast Ethernet.

FAT32 (32-bit File Allocation Table) — An enhanced version of FAT that accommodates the use of long filenames and smaller allocation units on a disk. FAT32 makes more efficient use of disk space than the original FAT and is therefore faster and can handle larger files.

FAT16 (16-bit File Allocation Table) — A file system designed for use with early DOS- and Windows-based computers that allocates file system space in 16-bit units. Compared to FAT32, FAT16 is less desirable because of its partition size, file naming, fragmentation, speed, and security limitations.

fault — The malfunction of one component of a system. A fault can result in a failure.

fault tolerance — The capacity for a system to continue performing despite an unexpected hardware or software malfunction.

feasibility study — A study that determines the costs and benefits of a project and attempts to predict whether the project will result in a favorable outcome (for example, whether it will achieve its goal without imposing excessive cost or time burdens on the organization).

Federal Communications Commission (FCC) — The regulatory agency that sets standards and policy for telecommunications transmission and equipment in the United States.

Fiber Distributed Data Interface (FDDI) — A networking standard originally specified by ANSI in the mid-1980s and later refined by ISO. FDDI uses a dual fiber-optic ring to transmit data at speeds of 100 Mbps. It was commonly used as a backbone technology in the 1980s and early 1990s, but lost favor as fast Ethernet technologies emerged in the mid-1990s. FDDI provides excellent reliability and security.

fiber-optic cable — A form of cable that contains one or several glass fibers in its core. Data are transmitted via pulsing light sent from a laser or light-emitting diode through the central fiber (or fibers). Outside the central fiber, a layer of glass called cladding acts as a mirror, reflecting light back to the core in patterns that vary depending on the transmission mode. Outside the cladding, a plastic buffer protects the core and absorbs any light that might escape. Outside the buffer, strands of Kevlar provide further protection from stretching and damage. A plastic jacket surrounds the Kevlar strands.

fiber-optic modem (FOM) — A demultiplexer used on fiber networks that employ wave division multiplexing. The fiber-optic modem separates the multiplexed signals into individual signals according to their different wavelengths.

Fibre Channel — A distinct network transmission method that relies on fiber-optic media and its own, proprietary protocol. Fibre Channel is capable of 1-Gbps (and soon, 2-Gbps) throughput.

file server — A specialized server that enables clients to share applications and data across the network.

file services — The function of a file server that allows users to share data files, applications, and storage areas.

file system — An operating system's method of organizing, managing, and accessing its files through logical structures and software routines.

File Transfer Protocol (FTP) — An application layer protocol in the TCP/IP protocol suite that manages file transfers between TCP/IP hosts.

file-infected virus — A virus that attaches itself to executable files. When the infected executable file runs, the virus copies itself to memory. Later, the virus will attach itself to other executable files.

filtering database — A collection of data created and used by a bridge that correlates the MAC addresses of connected workstations with their locations. A filtering database is also known as a forwarding table.

firewall — A specialized device (typically a router, but possibly only a PC running special software) that selectively filters or blocks traffic between networks. A firewall may be strictly hardware-based, or it may involve a combination of hardware and software.

firmware — A combination of hardware and software. The hardware component of firmware is a read-only memory (ROM) chip that stores data established at the factory and possibly changed by configuration programs that can write to ROM.

flashing — A security attack in which an Internet user sends commands to another Internet user's machine that cause the screen to fill with garbage characters. A flashing attack will cause the user to terminate his or her session.

flavor — Term used to refer to the different implementations of a particular UNIX-like system. For example, the different flavors of Linux include Red Hat, Caldera, and Mandrake.

flow control — A method of gauging the appropriate rate of data transmission based on how fast the recipient can accept data.

forest — In the context of Windows 2000 Server, a collection of domain trees that use different namespaces. A forest allows for trust relationships to be established between trees.

Format Prefix — A variable-length field at the beginning of an IPv6 address that indicates what type of address it is (for example, unicast, anycast, or multicast).

forwarding table — See *filtering database*.

fox and hound — Another term for the combination of devices known as a tone generator and a tone locator. The tone locator is considered the hound because it follows the tone generator (the fox).

fractional T1 — An arrangement that allows organizations to use only some channels on a T1 line and pay for only the channels actually used.

frame — A package for data that includes not only the raw data, or "payload," but also the sender's and receiver's network addresses and control information.

Frame Check Sequence (FCS) — The field in a data frame responsible for ensuring that data carried by the frame arrives intact. FCS uses an algorithm, such as CRC, to accomplish this verification.

frame relay — An updated, digital version of X.25 that relies on packet switching. Because it is digital, frame relay supports higher bandwidth than X.25, offering a maximum of 45-Mbps throughput. It provides the basis for much of the world's Internet connections. On network diagrams, the frame relay system is often depicted as a cloud.

FreeBSD — An open source software implementation of the Berkeley Software Distribution version of the UNIX system.

freely distributable — A term used to describe software with a very liberal copyright. Often associated with open source software.

frequency — The number of times that a signal's amplitude changes over a fixed period of time, expressed in cycles per second, or hertz (Hz).

frequency modulation (FM) — A method of data modulation in which the frequency of the carrier signal is modified by the application of the data signal.

full backup — A backup in which all data on all servers are copied to a storage medium, regardless of whether the data are new or changed.

full-duplex — A type of transmission in which signals may travel in both directions over a medium simultaneously. May also be called, simply, "duplex."

fully qualified domain name (FQDN) — In TCP/IP addressing, the combination of a host and domain name that together uniquely identify a device.

Gantt chart — A popular method of depicting when projects begin and end along a horizontal timeline.

gateway — A combination of networking hardware and software that connects two dissimilar types of networks. Gateways perform connectivity, session management, and data translation, so they must operate at multiple layers of the OSI Model.

Gateway Services for NetWare (GSNW) — A Windows 2000 service that acts as a translator between the Windows 2000 and NetWare client redirector services. With GSNW installed, a Windows 2000 server can access files and other shared resources on any NetWare server on a network.

General Public License — The copyright that applies to freely distributable versions of UNIX and specifies that the source code must be made available to anyone receiving the system.

ghosts — Frames that are not actually data frames, but rather aberrations caused by a repeater misinterpreting stray voltage on the wire. Unlike true data frames, ghosts have no starting delimiter.

giants — Packets that exceed the medium's maximum packet size. For example, any Ethernet packet that is larger than 1518 bytes is considered a giant.

global group — A group on a Windows 2000 network that allows members of one domain to access resources within that domain as well as resources from other domains in the same forest.

globally unique identifier (GUID) — A 128-bit number generated and assigned to an object upon its creation in the Windows 2000 Active Directory. Network applications and services use an object's GUID to communicate with it.

globbing — A form of filename substitution, similar to the use of wildcards in Windows and DOS.

GNU — The name given to the free software project to implement a complete source code implementation of UNIX, the collection of UNIX-inspired utilities and tools that are included with Linux distributions and other free software UNIX systems. The acronym within an acronym stands for "GNUs Not UNIX."

gopher — A text-based utility that allows you to navigate through a series of menus to find and read specific files.

grandfather-father-son — A backup rotation scheme that uses daily (son), weekly (father), and monthly (grandfather) backup sets.

graphical user interface (GUI) — A pictorial representation of computer functions and elements that, in the case of network operating systems, enables administrators to more easily manage files, users, groups, security, printers, and other issues.

group — A means of collectively managing users' permissions and restrictions applied to shared resources. Groups form the basis for resource and account management for every type of network operating system, not just Windows 2000 Server. Many network administrators create groups according to department or, even more specifically, according to job function within a department.

Guest — A user account with very limited privileges that is created during the installation of a network operating system.

hacker — A person who masters the inner workings of operating systems and utilities in an effort to better understand them. A hacker is distinguished from a cracker in that a cracker will attempt to exploit a network's vulnerabilities for malicious purposes.

half-duplex — A type of transmission in which signals may travel in both directions over a medium, but in only one direction at a time.

handshake protocol — One of several protocols within SSL, and perhaps the most significant. As its name implies, the handshake protocol allows the client and server to authenticate (or introduce) each other and establishes terms for how they will securely exchange data during an SSL session.

hard disk redundancy — See *Redundant Array of Inexpensive Disks (RAID).*

Hardware Compatibility List (HCL) — A list of computer components proven to be compatible with Windows 2000 Server. The HCL appears on the same CD as your Windows 2000 Server software and on Microsoft's Web site.

head-end — A cable company's central office, which connects cable wiring to many nodes before it reaches customers' sites.

hertz (Hz) — A measure of frequency equivalent to the number of amplitude cycles per second.

heuristic scanning — A type of virus scanning that attempts to identify viruses by discovering "virus-like" behavior.

hierarchical file system — The organization of files and directories (or folders) on a disk partition in which directories may contain files and other directories. When displayed graphically, this organization resembles a tree-like structure.

hierarchical hybrid topology — A network topology in which devices are divided into separate layers according to their priority or function.

High-Performance File System (HPFS) — A file system designed for IBM's OS/2 operating system that offers greater efficiency and reliability than does FAT. HPFS is rarely used but can be supported by Windows 2000 servers.

High-Speed Token Ring (HSTR) — A standard for Token Ring networks that operate at 100 Mbps.

hop — A term used to describe each trip data take from one connectivity device to another.

host — 1) A computer connected to a network that uses the TCP/IP protocol. 2) A type of computer that enables resource sharing by other computers on the same network.

host file — A text file that associates TCP/IP host names with IP addresses. On Windows 9x, NT, and 2000 platforms, the host file is called "lmhosts." On UNIX platforms the file is called "hosts" and is located in the /etc directory.

host name — A symbolic name that describes a TCP/IP device.

hosts — Name of the DNS host file found on a UNIX computer. The hosts file is usually found in the /etc directory.

hot swappable — A characteristic that enables identical components to be interchanged (or swapped) while a machine is still running (hot). Once installed, hot swappable components automatically assume the functions of their counterpart if it suffers a fault.

HOWTO — A series of brief, highly focused documents giving Linux system details. The people responsible for the Linux Documentation Project centrally coordinate the HOWTO papers (see *www.linuxhq.com/ldp/howto/HOWTO-INDEX/howtos.html*).

HP-UX — Hewlett-Packard's proprietary implementation of the UNIX system.

HTTPS — The URL prefix that indicates that a Web page requires its data to be exchanged between client and server using SSL encryption. HTTPS uses the TCP port number 443, rather than port 80 (the port that normal HTTP uses).

hub — A multiport repeater containing multiple ports to interconnect multiple devices. Unless they are used on a peer-to-peer network, hubs also contain an uplink port, one port that connects to a network's backbone. Hubs regenerate digital signals.

Hurd — The kernel in the GNU operating system. While many UNIX and Linux systems include GNU utilities such as the EMACS editor or the GNU C compiler, the Hurd is the only operating system kernel that can currently be called a GNU kernel.

hybrid fiber-coax (HFC) — A link that consists of fiber cable connecting the cable company's offices to a node location near the customer and coaxial cable connecting the node to the customer's house. HFC upgrades to existing cable wiring are required before current TV cable systems can serve as WAN links.

hybrid topology — A complex combination of the simple physical topologies.

Hypertext Markup Language (HTML) — The language that defines formatting standards for Web documents.

Hypertext Transport Protocol (HTTP) — The language that Web clients and servers use to communicate. HTTP forms the backbone of the Web.

i-node — A UNIX file system information storage area that holds all details about a file. This information includes the size, access rights, date and time of creation, and a pointer to the actual contents of the file.

ICA (Independent Computing Architecture) client — A remote access client developed by Citrix Systems, Inc. that enables remote users to use virtually any LAN application over any type of connection, public or private. The ICA client is especially well suited to slower connections, as it exchanges only keystrokes, mouse clicks, and screen updates with the server. The ICA client requires that Citrix's server software run on the access server."

IEEE (Institute of Electrical and Electronic Engineers) — An international society composed of engineering professionals. Its goals are to promote development and education in the electrical engineering and computer science fields.

IEEE 802.3 frame — A popular Ethernet frame type used on IPX/SPX networks. The defining characteristics of its data portion are the source and destination service access points that belong to the Logical Link Control layer, a sublayer of the Data Link layer. Also called LLC or, in Novell lingo, Ethernet 802.2.

IEEE 802.3 SNAP frame — A rarely used Ethernet frame type that is an adaptation of IEEE 802.3 and Ethernet II. SNAP stands for Sub-Network Access Protocol. The SNAP portion of the frame contains the three Logical Link Control fields (DSAP, SSAP, and Control). The Organization ID (OUI) field provides a method of identifying the type of network on which the frame is running. In addition, Ethernet SNAP frames carry Ethernet type information, just as an Ethernet II frame does.

ifconfig — A TCP/IP configuration and management utility used with UNIX systems (similar to the ipconfig utility used on Windows NT and 2000 systems).

incremental backup — A backup in which only data that have changed since the last backup are copied to a storage medium.

indirect infrared transmission — A type of infrared transmission in which signals bounce off walls, ceilings, and any other objects in their path. Because indirect infrared signals are not confined to a specific pathway, they are not very secure.

Industry Standard Architecture (ISA) — The original PC bus, developed in the early 1980s to support an 8-bit and later 16-bit data transfer capability. Although an older technology, ISA buses are still used to connect serial devices, such as mice or modems, in new PCs.

infrared — A type of data transmission in which infrared light signals are used to transmit data through space, similar to the way a television remote control sends signals across the room. Networks may use two types of infrared transmission: direct or indirect.

integrity — The soundness of a network's files, systems, and connections. To ensure integrity, you must protect your network from anything that might render it unusable, such as corruption, tampering, natural disasters, and viruses.

integrity checking — A method of comparing the current characteristics of files and disks against an archived version of these characteristics to discover any changes. The most common example of integrity checking involves a checksum.

intelligent hub — A hub that possesses processing capabilities and can therefore interpret and manage data traffic, rather than simply regenerating signals as a simple hub would do.

Internet — A complex WAN that connects LANs around the globe.

Internet Control Message Protocol (ICMP) — A core protocol in the TCP/IP suite that notifies the sender that something has gone wrong in the transmission process and that packets were not delivered.

Internet Corporation for Assigned Names and Numbers (ICANN) — The non-profit corporation currently designated by the U.S. government to maintain and assign IP addresses.

Internet Key Exchange (IKE) — The first phase of IPSec authentication, which accomplishes key management. IKE is a service that runs on UDP port 500. Once IKE has established the rules for the type of keys two nodes will use, IPSec invokes its second phase, encryption.

Internet Mail Access Protocol (IMAP) — A mail storage and manipulation protocol that depends on SMTP's transport system and improves upon the shortcomings of POP. The most current version of IMAP is version 4 (IMAP4). IMAP4 can (and eventually will) replace POP without the user having to change e-mail programs. The single biggest advantage IMAP4 has relative to POP is that it allows users to store messages on the mail server, rather than always having to download them to the local machine.

Internet Protocol (IP) — A core protocol in the TCP/IP suite that belongs to the Internet layer of the TCP/IP model and provides information about how and where data should be delivered. IP is the subprotocol that enables TCP/IP to internetwork.

Internet services — Services that enable a network to communicate with the Internet, including World Wide Web servers and browsers, file transfer capabilities, Internet addressing schemes, security filters, and a means for directly logging on to other computers.

Internet telephony — The provision of telephone service over the Internet.

internetwork — To traverse more than one LAN segment and more than one type of network through a router.

Internetwork Packet Exchange (IPX) — A core protocol of the IPX/SPX suite that operates at the Network layer of the OSI Model and provides routing and internetwork services, similar to IP in the TCP/IP suite.

Internetwork Packet Exchange/Sequenced Packet Exchange (IPX/SPX) — A protocol originally developed by Xerox, then modified and adopted by Novell in the 1980s for the NetWare network operating system.

interrupt — A wire through which a device issues voltage, thereby signaling a request for the processor's attention.

interrupt request (IRQ) — A message sent to the computer that instructs it to stop what it is doing and pay attention to something else. IRQ is often used (informally) to refer to the interrupt request number.

interrupt request number (IRQ number) — The unique number assigned to each interrupt request in a computer. Interrupt request numbers range from 0 to 15, and many PC devices reserve specific numbers for their use alone.

IntraNetWare — Another term for NetWare version 4.11, the version in which support for Internet services was first introduced.

intrusion detection — The process of monitoring the network for unauthorized access to its devices.

IP address — A logical address used in TCP/IP networking. This unique 32-bit number is divided into four groups of octets, or 8-bit bytes, that are separated by periods.

IP datagram — The IP portion of a TCP/IP frame that acts as an envelope for data, holding information necessary for routers to transfer data between subnets.

IP next generation (IPng) — See *IP Version 6*.

IP Security Protocol (IPSec) — A Layer 3 protocol that defines encryption, authentication, and key management for TCP/IP transmissions. IPSec is an enhancement to IPv4 and native to IPv6. IPSec is unique among authentication methods in that it adds security information to the header of all IP packets.

IP spoofing — A security attack in which an outsider obtains internal IP addresses, then uses those addresses to pretend that he or she has authority to access a private network from the Internet.

IP version 6 (IPv6) — A new standard for IP addressing that will replace the current IP version 4 (IPv4). Most notably, IPv6 uses a newer, more efficient header in its packets and allows for 128-bit source and destination IP addresses. The use of longer addresses will allow for more total IP addresses to be in circulation.

ipconfig — The TCP/IP configuration and management utility for use with Windows NT or Windows 2000 systems.

IPX address — An address assigned to a device on an IPX/SPX network.

ISDN (Integrated Services Digital Network) — An international standard, established by the ITU, for transmitting data over digital lines. Like PSTN, ISDN uses the telephone carrier's lines and dial-up connections, but it differs from PSTN in that it exclusively uses digital lines and switches.

ISO (International Organization for Standardization) — A collection of standards organizations representing 130 countries with headquarters located in Geneva, Switzerland. Its goal is to establish international technological standards to facilitate the global exchange of information and barrier-free trade.

ITU (International Telecommunication Union) — A United Nations agency that regulates international telecommunications, including radio and TV frequencies, satellite and telephony specifications, networking infrastructure, and tariffs applied to global communication. It also provides developing countries with technical expertise and equipment to advance these nations' technological bases.

jabber — A device that handles electrical signals improperly, usually affecting the rest of the network. A network analyzer will detect a jabber as a device that is always retransmitting, effectively bringing the network to a halt. A jabber usually results from a bad NIC. Occasionally, it can be caused by outside electrical interference.

jamming — A part of CSMA/CD in which, upon detecting a collision, a station issues a special 32-bit sequence to indicate to all nodes on an Ethernet segment that its previously transmitted frame has suffered a collision and should be considered faulty.

jumper — A small, removable piece of plastic that contains a metal receptacle that fits over a pair of pins on a circuit board to complete a circuit between those two pins. By moving the jumper from one set of pins to another set of pins, you can modify the board's circuit, thereby giving it different instructions on how to operate.

Kerberos — A cross-platform authentication protocol that uses key encryption to verify the identity of clients and to securely exchange information once a client logs onto a system. It is an example of a private key encryption service.

kernel — The core of an operating system, such as UNIX or NetWare. The kernel, which is loaded into memory as the computer starts, oversees all critical server processes.

kernel modules — Portions of the Linux kernel that you can load and unload to add or remove functionality on a running Linux system.

key — A series of characters that is combined with a block of data during that data's encryption. In order to decrypt the resulting data, the recipient must also possess the key.

key distribution center (KDC) — In Kerberos terminology, the server that runs the authentication service and the ticket granting service in order to issue keys and tickets to clients. On a Windows 2000 network, a user's domain controller serves as his KDC.

key management — The method whereby two nodes using key encryption agree on common parameters for the keys they will use in order to encrypt data.

key pair — The combination of a public and private key used to decipher data that has been encrypted using public key encryption.

LAN — See *local area network*.

LAN Emulation (LANE) — A method for transporting Token Ring or Ethernet frames over ATM networks. LANE encapsulates incoming Ethernet or Token Ring frames, then converts them into ATM cells for transmission over an ATM network.

LAN topology — The physical layout, or pattern, of nodes on a local area network (LAN).

LANalyzer — Novell's network monitoring software package. LANalyzer can act as a standalone program on a Windows 9x or 2000 workstation or as part of the ManageWise suite of network management tools on a NetWare server. LANalyzer offers the following capabilities: discovery of all network nodes on a segment, continuous monitoring of network traffic, alarms that are tripped when traffic conditions meet preconfigured thresholds (for example, if usage exceeds 70%), and the capturing of traffic to and from all or selected nodes.

late collisions — Collisions that take place outside the normal window in which collisions are detected and redressed. Late collisions are usually caused by a defective station (such as a card, or transceiver) that is transmitting without first verifying line status or by failure to observe the configuration guidelines for cable length, which results in collisions being recognized too late.

latency — The delay between the transmission of a signal and its receipt.

layer — (1) In the context of hierarchical topologies, the division between one set of devices and another set of devices on a network; (2) A portion of the OSI Model that corresponds to specific processes involved in data communication between two computers.

Layer 2 Forwarding (L2F) — A Layer 2 protocol similar to PPTP that provides tunneling for other protocols and can work with the authentication methods used by PPP. L2F was developed by Cisco Systems and requires special hardware on the host system end. It can encapsulate protocols to fit more than just the IP format, unlike PPTP.

Layer 2 Tunneling Protocol (L2TP) — A Layer 2 tunneling protocol developed by a number of industry consortia. L2TP is an enhanced version of L2F. Like L2F, it supports multiple protocols; unlike L2F, it does not require costly hardware upgrades to implement. L2TP is optimized to work with the next generation of IP (IPv6) and IPSec (the Layer 3 IP encryption protocol).

Layer 3 switch — A switch capable of interpreting data at Layer 3 (Network layer) of the OSI Model.

Layer 4 switch — A switch capable of interpreting data at Layer 4 (Transport layer) of the OSI Model.

lease — The agreement between a DHCP server and client on how long the client will borrow a DHCP-assigned IP address. As network administrator, you configure the duration of the lease (in the DHCP service) to be as short or long as necessary, from a matter of minutes to forever.

leased lines — Permanent dedicated connections established through a public telecommunications carrier and billed to customers on a monthly basis.

license tracking — Determining how many copies of a single application are currently in use on the network.

Lightweight Directory Access Protocol (LDAP) — A standard protocol for accessing network directories.

line noise — Fluctuations in voltage levels caused by other devices on the network or by electromagnetic interference.

Linux — A freely distributable implementation of the UNIX system. Finnish computer scientist Linus Torvalds originally developed it.

LLC frame — See *IEEE 802.3 frame*.

lmhosts — A host file on a Windows-based computer that maps IP addresses to host names and aliases.

load balancing — An automatic distribution of traffic over multiple links, hard disks, or processors intended to optimize responses.

Lobe Attachment Module (LAM) — A device that attaches to a CAU to expand the capacity of that device. LAMs typically allow up to 20 devices to plug into each CAU receptacle.

local account — A type of user account on a Windows 2000 network that has rights to the resources managed by the server the user has logged onto.

local area network (LAN) — A network of computers and other devices that is confined to a relatively small space, such as one building or even one office.

local collisions — Collisions that occur when two or more stations are transmitting simultaneously. Excessively high collision rates within the network can usually be traced to cable or routing problems.

local computer — The computer on which you are actually working (as opposed to a remote computer).

local loop — The part of a phone system that connects a customer site with a public carrier's POP. Some WAN transmission methods, such as ISDN, are suitable for only the local loop portion of the network link.

LocalTalk — A logical topology designed by Apple Computer, Inc. especially for networking Macintosh computers. LocalTalk uses the CSMA/CA network access method, and its throughput is limited to a maximum of 230 Kbps. Because of its throughput limitations, LocalTalk has been replaced by Ethernet on most modern Macintosh-based networks.

logical address — See *Network layer addresses*.

Logical Link Control (LLC) sublayer — The upper sublayer in the Data Link layer. The LLC provides a common interface and supplies reliability and flow control services.

logical topology — A networking technology defined by its Data Link layer data packaging and Physical layer signaling techniques. Also known as network transport system or access method.

loopback address — An IP address reserved for communicating from a node to itself (used mostly for testing purposes). The value of the loopback address is always 127.0.0.1.

loopback plug — A connector used for troubleshooting that plugs into a port (for example, a serial, parallel, or RJ-45 port) and crosses over the transmit line to the receive line, allowing outgoing signals to be redirected back into the computer for testing.

MAC address — A number that uniquely identifies a network node. The manufacturer hard-codes the MAC address on the NIC. This address is composed of the Block ID and Device ID.

macro viruses — A newer type of virus that takes the form of a word-processing or spreadsheet program macro, which may execute when a word-processing or spreadsheet program is in use.

MacTCP – A version of the TCP/IP protocol supplied with LocalTalk.

mail services — Network services that manage the storage and transfer of e-mail between users on a network. In addition to sending, receiving, and storing mail, mail services can include intelligent e-mail routing capabilities, notification, scheduling, indexing, document libraries, and gateways to other mail servers.

MAN — See *metropolitan area network*.

managed hub — See *intelligent hub*.

management services — Network services that centrally administer and simplify complicated management tasks on the network. Examples of management services include license tracking, security auditing, asset management, addressing management, software distribution, traffic monitoring, load balancing, and hardware diagnosis.

manual pages (man pages) — UNIX online documentation. This documentation describes the use of the commands and the programming interface to the UNIX system.

Media Access Control (MAC) sublayer — The lower sublayer of the Data Link layer. The MAC appends the physical address of the destination computer onto the frame.

media access unit (MAU) — The type of transceiver used on a Thicknet network to connect network nodes to the backbone.

media filter — A device that enables two types of cables or connectors to be linked.

member server — A type of server on a Windows 2000 network that does not hold directory information and therefore cannot authenticate users.

memory range — A hexadecimal number that indicates the area of memory that the network adapter and CPU will use for exchanging, or buffering, data. As with IRQs, some memory ranges are reserved for specific devices—most notably, the system board.

mesh network — An enterprise-wide topology in which routers are interconnected with other routers so that at least two pathways connect each node.

mesh WAN topology — A WAN topology that consists of many directly interconnected locations forming a complex mesh.

message switching — A type of switching in which a connection is established between two devices in the connection path; one device transfers data to the second device, then breaks the connection. The information is stored and forwarded from the second device once a connection between that device and a third device on the path is established.

metropolitan area network (MAN) — A network that connects clients and servers in multiple buildings within a limited geographic area. For example, a network connecting multiple city government buildings around the city's center.

MIB (management information base) — A collection of data used by management programs (which may be part of the network operating system or a third-party program) to analyze network performance and problems.

MicroChannel Architecture (MCA) — IBM's proprietary 32-bit bus for personal computers, introduced in 1987 and later replaced by the more standard EISA and PCI buses.

Microsoft Certified Systems Engineer (MCSE) — A professional certification established by Microsoft that demonstrates in-depth knowledge about Microsoft's products, including Windows 98 and Windows 2000.

Microsoft Management Console (MMC) — A graphical network management interface used with Windows 2000 Server.

Microsoft Message Queueing (MSMQ) — An API used in a network environment. MSMQ stores messages sent between nodes in queues then forwards them to their destination based on when the link to the recipient is available.

middleware — Software that sits between the client and server in a 3-tier architecture. Middleware may be used as a messaging service between clients and servers, as a universal query language for databases, or as means of coordinating processes between multiple servers that need to work together in servicing clients.

milestone — A reference point that marks the completion of a major task or group of tasks in a project and contributes to measuring the project's progress.

mirroring — See *server mirroring*.

modem — A device that modulates analog signals into digital signals at the transmitting end for transmission over telephone lines, and demodulates digital signals into analog signals at the receiving end.

modular hub — A type of hub that provides a number of interface options within one chassis. Similar to a PC, a modular hub contains a system board and slots accommodating different adapters. These adapters may connect to other types of hubs, routers, WAN links, or to both Token Ring and Ethernet network backbones. They may also connect the modular hub to management workstations or redundant components, such as an extra power supply.

modular router — A router with multiple slots that can hold different interface cards or other devices so as to provide flexible, customizable network interoperability.

modulation — A technique for formatting signals in which one property of a simple, carrier wave is modified by the addition of a data signal during transmission.

Monitor — An NLM that enables the system administrator to view server parameters such as protocols, bindings, system resources, and loaded modules. In many cases, it also allows the system administrator to modify these parameters.

multi-master replication — The technique of replicating an Active Directory database to multiple domain controllers so they each have the same data and the same privileges to modify that data. Multi-master replication is used within a domain tree.

multicast address — A type of address in the IPv6 that represents multiple interfaces, often on multiple nodes. An IPv6 multicast address begins with the following hexadecimal field: FF0*x*, where *x* is a character that identifies the address's group scope.

multicasting — A means of transmission in which one device sends data to a specific group of devices (not the entire network segment) in a point-to-multipoint fashion. Multicasting can be used for teleconferencing or videoconferencing over the Internet, for example.

multimeter — A simple instrument that can measure multiple characteristics of an electric circuit, including its resistance and voltage.

multimode fiber — A type of fiber-optic cable that contains a core with a diameter between 50 and 100 microns, over which many pulses of light generated by a light emitting diode (LED) travel at different angles. Because light is being reflected many different ways in a multimode fiber cable, the waves become less easily distinguishable the longer they travel. Thus, multimode fiber is best suited for shorter distances than single-mode fiber.

multiplexer (mux) — A device that separates a medium into multiple subchannels and issues signals to each of those subchannels.

multiplexing — A form of transmission that allows multiple signals to simultaneously travel over one medium.

multiprocessing — The technique of splitting tasks among multiple processors to expedite the completion of any single instruction.

multiprotocol network — A network that uses more than one protocol.

Multistation Access Unit (MAU) — A device on a Token Ring network that regenerates signals; equivalent to a hub.

multitasking — The ability of a processor to perform multiple activities in a brief period of time (often seeming simultaneous to the user).

n-series connector (n connector) — A type of connector used on Thicknet networks in which a screw-and-barrel arrangement securely connects coaxial cables to devices.

name server — A server that contains a database of TCP/IP host names and their associated IP addresses. A name server supplies a resolver with the requested information. If it cannot resolve the IP address, the query passes to a higher-level name server.

name space — The database of Internet IP addresses and their associated names distributed over DNS name servers worldwide.

narrowband — A type of radiofrequency transmission in which signals travel over a single frequency. The same method is used by radio and TV broadcasting stations, and signals can be easily intercepted and decoded.

nbtstat — A TCP/IP troubleshooting utility that provides information about NetBIOS names and their addresses. If you know the NetBIOS name of a workstation, you can use nbtstat to determine its IP address.

NDS eDirectory — Novell's integration tool for Windows 2000 networks. It works with the NetWare 5.x operating systems and Windows 2000 servers to enable the Windows 2000 domains to appear as container objects in NWAdmin.

NDS tree — A logical representation of how resources are grouped by NetWare in the enterprise.

needs assessment — The process of clarifying the reasons and objectives for a proposed change so as to determine whether the change is worthwhile and necessary and to elucidate the scope and nature of the proposed change.

negative frame sequence checks — The result of the cyclic redundancy checksum (CRC) generated by the originating node not matching the checksum calculated from the data received. It usually indicates noise or transmission problems on the LAN interface or cabling. A high number of (non-matching) CRCs usually results from excessive collisions or a station transmitting bad data.

NetBIOS — See *Network Basic Input Output System*.

NetBIOS Enhanced User Interface (NetBEUI) — Microsoft's adaptation of the IBM NetBIOS protocol. NetBEUI expands on NetBIOS by adding an Application layer component. NetBEUI is a fast and efficient protocol that consumes few network resources, provides excellent error correction and requires little configuration.

netstat — A TCP/IP troubleshooting utility that displays statistics and the state of current TCP/IP connections. It also displays ports, which can signal whether services are using the correct ports.

NetWare 3.x — The group of NetWare versions that includes versions 3.0, 3.1, and 3.2.

NetWare 4.x — The group of NetWare versions that includes versions 4.0, 4.1, and 4.11.

NetWare 5.x — The group of NetWare versions that includes versions 5.0, 5.1, and 5.11.

NetWare Administrator utility (NWAdmin) — The graphical NetWare utility that allows administrators to manage objects in the NDS tree from a Windows workstation.

NetWare Core Protocol (NCP) — One of the core protocols of the IPX/SPX suite. NCP handles requests for services, such as printing and file access, between clients and servers.

NetWare Directory Services (NDS) — A system of managing multiple servers and their resources, including users, volumes, groups, profiles, and printers. The NDS model is similar to Active Directory in Windows 2000. In NDS, every networked resource is treated as a separate object with distinct properties.

NetWare loadable modules (NLMs) — Routines that enable the server to run programs and services. Each NLM consumes some of the server's memory and processor resources (at least temporarily). The kernel requires many NLMs to run NetWare's core operating system.

network — A group of computers and other devices (such as printers) that are connected by some type of transmission media, usually wire or cable.

network access method — See *access method*.

network adapter — A synonym for NIC (network interface card). The device that enables a workstation, server, printer, or other node to connect to the network. Network adapters belong to the Physical layer of the OSI Model.

network address — See *Network layer addresses*.

network address translation (NAT) — A technique in which private (or hidden) IP addresses are assigned a public IP address by an IP gateway, thus masking their true origin.

network analyzer — A portable, hardware-based tool that a network manager connects to the network expressly to determine the nature of network problems. Network analyzers can typically interpret data up to Layer 7 of the OSI Model.

network architect — A professional who designs networks, performing tasks that range from choosing basic components (such as cabling type) to figuring out how to make those components work together (by, for example, choosing the correct protocols).

network attached storage (NAS) — A device or set of devices attached to a client/server network that is dedicated to providing highly fault-tolerant access to large quantities of data. NAS depends on traditional network transmission methods such as Ethernet.

Network Basic Input Output System (NetBIOS) — A protocol designed by IBM to provide Transport and Session layer services for applications running on small, homogeneous networks.

network interface card (NIC) — The device that enables a workstation to connect to the network and communicate with other computers. NICs are manufactured by several different companies and come with a variety of specifications that are tailored to the workstation's and the network's requirements.

Network layer — The third layer in the OSI Model. The Network layer translates network addresses into their physical counterparts and decides how to route data from the sender to the receiver.

Network layer addresses — Addresses that reside at the Network level of the OSI Model, follow a hierarchical addressing scheme, and can be assigned through operating system software.

Network Monitor (NetMon) — A software-based network monitoring tool that comes with Windows NT Server 4.0 or Windows 2000. Its capabilities include capturing network data traveling from one or many segments, capturing frames sent by or to a specified node, reproducing network conditions by transmitting a selected amount and type of data, detecting any other running copies of NetMon, and generating statistics about network activity.

network monitor — A software-based tool that continually monitors traffic on the network from a server or workstation attached to the network. Network monitors typically can interpret up to Layer 3 of the OSI Model.

Network News Transfer Protocol (NNTP) — The protocol that supports the process of reading newsgroup messages, posting new messages, and transferring news files between news servers.

network operating system (NOS) — The software that runs on a server and enables the server to manage data, users, groups, security, applications, and other networking functions. The most popular network operating systems are Microsoft's Windows NT, Windows 2000, UNIX, and Novell's NetWare.

Network Termination 1 (NT1) — A device used on ISDN networks that connects the incoming twisted-pair wiring with the customer's ISDN terminal equipment.

Network Termination 2 (NT2) — An additional connection device required on PRI to handle the multiple ISDN lines between the customer's network termination connection and the local phone company's wires.

Network Time Protocol (NTP) — A simple TCP/IP protocol that is used to synchronize the clocks of computers on a network. NTP belongs to the Application layer of the TCP/IP Model and depends on UDP.

network transport system — See *logical topology*.

network virus — A type of virus that takes advantage of network protocols, commands, messaging programs, and data links to propagate itself. Although all viruses could theoretically travel across network connections, network viruses are specially designed to attack network vulnerabilities.

Network+ (Net+) — Professional certification established by CompTIA that verifies broad, vendor-independent networking technology skills such as an understanding of protocols, topologies, networking hardware, and network troubleshooting.

New Technology File System (NTFS) — A file system developed by Microsoft for use with its Windows NT and Windows 2000 operating systems. NTFS integrates reliability, compression, the ability to handle massive files, system security, and fast access. Most Windows 2000 Server partitions employ either FAT32 or NTFS.

newsgroups — An Internet service similar to e-mail that provides a means of conveying messages, but in which information is distributed to a wide group of users at once rather than from one user to another.

NFS — Network File System. A client/server application that allows you to view, store and update files on a remote computer as though they were on your own computer. Can be used to install Linux.

node — A computer or other device connected to a network which has a unique address and is capable of sending or receiving data.

noise — Unwanted signals, or interference, from sources near network cabling, such as electrical motors, power lines and radar.

NOS — See *network operating system*.

Novell proprietary 802.3 frame — The original NetWare Ethernet frame type and the default frame type for networks running NetWare versions lower than 3.12. It supports only the IPX/SPX protocol. Sometimes called 802.3 "raw," because its data portion contains no control bits.

nslookup — A TCP/IP utility on Windows NT, Windows 2000, and UNIX systems that allows you to look up the DNS host name of a network node by specifying its IP address, or vice versa. This ability is useful for verifying that a host is configured correctly and for troubleshooting DNS resolution problems.

NWConv — A utility provided with Windows 2000 that converts (migrates) an existing NetWare server's user account, file, and other information to a Windows 2000 server.

object — A representation of a thing or person associated with the network that belongs in the NOS directory. Objects include users, printers, groups, computers, data files, and applications.

object class — See *Class*.

octet — One of the four 8-bit bytes that are separated by periods and together make up an IP address.

ohmmeter—A device used to measure resistance in an electrical circuit.

online backup — A technique in which data are backed up to a central location over the Internet.

online UPS — A power supply that uses the A/C power from the wall outlet to continuously charge its battery, while providing power to a network device through its battery.

open shortest path first (OSPF) — A routing protocol that makes up for some of the limitations of RIP and can coexist with RIP on a network.

open source software — Term used to describe software that is distributed without any restriction and whose source code is freely available. See also *freely distributable*.

Open Systems Interconnection (OSI) Model — A model for understanding and developing computer-to-computer communication developed in the 1980s by ISO. It divides networking architecture into seven layers: Physical, Data Link, Network, Transport, Session, Presentation, and Application.

optical loss — The degradation of a light signal on a fiber-optic network.

optical time domain reflector (OTDR) — A time domain reflector specifically made for use with fiber optic networks. It works by issuing a light-based signal on a fiber-optic cable and measuring the way in which the signal bounces back (or reflects) to the OTDR.

Orange Book — A rigorous security specification for computer operating systems published in 1985 by the U.S. Department of Defense.

Organizational unit (OU) — A container within an NOS directory used to group objects wih similar characteristics or priviledges.

OSI Model — See *Open Systems Interconnection Model.*

overhead — The nondata information that must accompany data in order for a signal to be properly routed and interpreted by the network.

owner — The person who takes responsibility for ensuring that project tasks are completed on time and within budgetary guidelines.

Packet Internet Groper (PING) — A TCP/IP troubleshooting utility that can verify that TCP/IP is installed, bound to the NIC, configured correctly, and communicating with the network. PING uses ICMP to send echo request and echo reply messages that determine the validity of an IP address.

packet switching — A type of switching in which data are broken into packets before they are transported. In packet switching, packets can travel any path on the network to their destination, because each packet contains a destination address and sequencing information.

packet-filtering firewall — A router that operates at the Data Link and Transport layers of the OSI Model, examining the header of every packet of data that it receives to determine whether that type of packet is authorized to continue to its destination. Packet-filtering firewalls are also called screening firewalls.

padding — Bytes added to the data (or information) portion of an Ethernet frame to make sure this field is at least 46 bytes in size. Padding has no effect on the data carried by the frame.

page file — A file on the hard disk that is used for virtual memory.

paging — The process of moving blocks of information, called pages, between RAM and into a page file on disk.

parallel backbone — The most robust enterprise-wide topology. This variation on the collapsed backbone arrangement consists of more than one connection from the central router or switch to each network segment.

parity — The mechanism used to verify the integrity of data by making the number of bits in a byte sum to either an odd or even number.

parity error checking — The process of comparing the parity of data read from a disk with the type of parity used by the system.

passive hub — A hub that simply amplifies and retransmits signals over the network.

patch — A correction, improvement, or enhancement to part of a software program, often distributed at no charge by software vendors to fix a bug in their code or to add slightly more functionality.

patch cable — A relatively short section (usually between 3 and 50 feet) of twisted-pair cabling, with connectors on both ends, that connects network devices to data outlets.

patch panel — A wall-mounted panel of data receptors into which cross-connect patch cables from the punch-down block are inserted.

PC Card — See *PCMCIA.*

PCMCIA — An interface developed in the early 1990s by the Personal Computer Memory Card International Association to provide a standard interface for connecting any type of device to a portable computer. PCMCIA slots may hold modem cards, network interface cards, external hard disk cards, or CD-ROM cards. PCMCIA cards are also known as PC Cards or credit card adapters.

peer-to-peer communication — A simple means of networking computers using a single cable. In peer-to-peer communication, no single computer has more authority than another and each computer can share its resources with other computers.

peer-to-peer network — A network in which computers communicate directly with other computers on a single segment of cable and share each others' data and devices. By default, no computer in a peer-to-peer network has more authority than another, and every computer can use resources from every other computer.

peer-to-peer topology — A WAN with single interconnection points for each location.

per seat — A Windows 2000 Server licensing mode that requires a license for every client capable of connecting to the Windows 2000 server.

per server — A Windows 2000 Server licensing mode that allows a limited number of clients to access the server simultaneously. (The number is determined by your Windows 2000 Server purchase agreement.) The restriction applies to the number of concurrent connections, rather than specific clients. Per server mode is the most popular choice for installing Windows 2000 Server.

Peripheral Component Interconnect (PCI) — A 32-, 64-, or 128-bit bus introduced in its original form in the 1990s. The PCI bus is the network adapter connection type used for nearly all new PCs. It's characterized by a shorter length than ISA, MCA, or EISA cards, but a much faster data transmission capability.

phase — A point or stage in a wave's progress over time.

physical address — See *MAC address.*

Physical layer — The lowest, or first, layer of the OSI Model. The Physical layer contains the physical networking media, such as cabling and connectors.

physical memory — The RAM chips installed on the computer's system board that provide dedicated memory to that computer.

physical topology — The physical layout of a network. A physical topology depicts a network in broad scope; it does not specify devices, connectivity methods, or addresses on the network. Physical topologies are categorized into three fundamental geometric shapes: bus, ring, and star. These shapes can be mixed to create hybrid topologies.

pilot network — A small-scale network that stands in for the larger network. A pilot network may be used to evaluate the effects of network changes or additions.

PING — See *Packet Internet Groper*.

pinging — The process of sending an echo request signal from one node on a TCP/IP network to another, using the PING utility.

pipe — The facility in a UNIX system that enables you to combine commands to form new commands. It is one of the most powerful facilities of the UNIX system.

pipeline — A series of two or more UNIX commands connected together with pipe symbols.

plain old telephone service (POTS) — See *PSTN*.

plenum — The area above the ceiling tile or below the subfloor in a building.

point of presence (POP) — The place where the two telephone systems meet—either a long-distance carrier with a local telephone company or a local carrier with an ISP's facility.

point-to-point — A data transmission that involves one transmitter and one receiver.

Point-to-Point Protocol (PPP) — A communications protocol that enables a workstation to connect to a server using a serial connection. PPP can support multiple Network layer protocols, can use both asynchronous and synchronous communications, and does not require much (if any) configuration on the client workstation.

Point-to-Point Tunneling Protocol (PPTP) — A Layer 2 protocol developed by Microsoft that encapsulates PPP so that any type of data can traverse the Internet masked as pure IP transmissions. PPTP supports the encryption, authentication, and LAN access services provided by RAS. Instead of users having to dial directly into an access server, they can dial into their ISP using PPTP and gain access to their corporate LAN over the Internet.

polymorphic virus — A type of virus that changes its characteristics (such as the arrangement of its bytes, size, and internal instructions) every time it is transferred to a new system, making it harder to identify.

POP — See *Post Office Protocol* or *point of presence*.

port — The address on a host where an application makes itself available to incoming data.

port number — A unique number associated with a process running on a computer. For example, 23 is the standard port number associated with the Telnet utility.

Post Office Protocol (POP) — A TCP/IP subprotocol that provides centralized storage for e-mail messages. In the postal service analogy, POP is like the post office that holds mail until it can be delivered.

predecessors — Tasks in a project that must be completed before other tasks can begin.

preemptive multitasking — The type of multitasking supported by NetWare, UNIX, and Windows 2000 Server that actually performs one task at a time, allowing one program to use the processor for a certain period of time, then suspending that program to allow another program to use the processor.

Presentation layer — The sixth layer of the OSI Model. The Presentation layer serves as a translator between the application and the network. Here data are formatted in a schema that the network can understand, with the format varying according to the type of network used. The Presentation layer also manages data encryption and decryption, such as the scrambling of system passwords.

Pretty Good Privacy (PGP) — A key-based encryption system for e-mail that uses a two-step verification process.

PRI (Primary Rate Interface) — A type of ISDN that uses 23 bearer channels and one 64-Kbps data channel as represented by the following notation: 23B + D. PRI is less commonly used by individual subscribers than BRI, but it may be used by businesses and other organizations needing more throughput.

principal — In Kerberos terminology, a user.

print services — The network service that allows printers to be shared by several users on a network.

printer queue — A logical representation of a networked printer's functionality. To use a printer, clients must have access to the printer queue.

private key encryption — A type of key encryption in which the sender and receiver have private keys, which only they know. Data encryption standard (DES), which was developed by IBM in the 1970s, is a popular example of a private key encryption technique. Private key encryption is also known as symmetric encryption.

process — A routine of sequential instructions that runs until it has achieved its goal. For example, a spreadsheet program is a process.

process management — Planning for and handling the steps involved in accomplishing a goal in a systematic way. Processes that might be managed during a project's implementation include change, support, training, transitioning, delegation, and problem resolution.

project management — The practice of managing resources, staff, budget, timelines, and other variables so as to complete a specific goal within given bounds.

project plan — The way in which details of a managed project (for example, the timeline and the significant tasks) are organized. Some project plans are created via special project planning software, such as Microsoft Project.

promiscuous mode — The feature of a network adapter card that allows a device driver to direct it to pick up all frames that pass over the network—not just those destined for the node served by the card.

proprietary UNIX — Any implementation of UNIX for which the source code is either unavailable or available only by purchasing a licensed copy from Caldera International and Tarantella, Inc. (costing as much as millions of dollars).

protected mode — A manner in which NetWare runs services in a separate memory area from the operating system. Running services in protected mode prevents one rogue routine from taking the server down. As a result, the service and its supporting routines cannot harm critical server processes.

protocol — The rules a network uses to transfer data. Protocols ensure that data is transferred whole, in sequence, and without error from one node on the network to another.

protocol analyzer — See *network analyzer.*

proxy server — A network host that runs a proxy service. Proxy servers may also be called gateways.

proxy service — A software application on a network host that acts as an intermediary between the external and internal networks, screening all incoming and outgoing traffic and providing one address to the outside world, instead of revealing the addresses of internal LAN devices.

PSTN (Public Switched Telephone Network) — The network of typical telephone lines that has been evolving for 100 years and still services most homes.

public key encryption — A form of key encryption in which data are encrypted using two keys: one is a key known only to a user, and the other is a key associated with the user and can be obtained from a public source, such as a public key server. Some examples of public key algorithms include RSA (named after its creators, Rivest, Shamir, and Adleman), Diffie-Hellman, and Elliptic-curve cryptography. Public key encryption is also known as asymmetric encryption.

public-key server — A publicly available host (such as an Internet host) that provides free access to a list of users' public keys (for use in public key encryption).

punch-down block — A panel of data receptors into which horizontal cabling from the workstations is inserted.

PVC (permanent virtual circuit) — A point-to-point connection over which data may follow any number of different paths, as opposed to a dedicated line that follows a predefined path. X.25, frame relay, and some forms of ATM use PVCs.

quality of service (QoS) — The result of standards for delivering data within a certain period of time after their transmission. For example, ATM networks can supply four QoS levels, from a "best effort" attempt for noncritical data to a guaranteed, real-time transmission for time-sensitive data.

radiofrequency (RF) — A type of transmission that relies on signals broadcast over specific frequencies, in the same manner as radio and TV broadcasts. RF may use narrowband or spread spectrum technology.

radiofrequency interference (RFI) — A kind of interference that may be generated by motors, power lines, televisions, copiers, fluorescent lights, or broadcast signals from radio or TV towers.

RAID — See *Redundant Array of Inexpensive Disks.*

RAID Level 0 — An implementation of RAID in which data are written in 64 KB blocks equally across all disks in the array.

RAID Level 1 — An implementation of RAID that provides redundancy through disk mirroring, in which data from one disk are automatically copied to another disk as the information is written.

RAID Level 3 — An implementation of RAID that uses disk striping for data and parity error correction code on a separate parity disk.

RAID Level 5 — The most popular, highly fault-tolerant, data storage technique in use today, RAID Level 5 writes data in small blocks across several disks. At the same time, it writes parity error checking information among several disks.

real-time — The term used to describe an operating system that at least one of the following includes two characteristics: the ability to respond to external events (for example, a change in temperature), and an ability to respond to those events deterministically—with predictable response time (for example, turning on a heating element within three microseconds).

reassembly — The process of reconstructing data units that have been segmented.

redirector — A service that runs on a client workstation and determines whether the client's request should be handled by the client or the server.

redundancy — The use of more than one identical component for storing, processing, or transporting data.

Redundant Array of Inexpensive Disks (RAID) — A server redundancy measure that uses shared, multiple physical or logical hard disks to ensure data integrity and availability. Some RAID designs also increase storage capacity and improve performance. See also *disk striping,* and *disk mirroring.*

regeneration — The process of retransmitting a digital signal. Regeneration, unlike amplification, repeats the pure signal, with none of the noise it has accumulated.

relative distinguished name (RDN) — An attribute of the object that identifies an object separately from its related container(s) and domain. For most objects, the relative distinguished name is the same as its common name (CN) in the distinguished name convention.

release — The act of terminating a DHCP lease.

remote access — A method for connecting and logging onto a LAN from a workstation that is remote, or not physically connected, to the LAN. Remote access can be accomplished one of three ways: by using a modem to dial directly into the LAN; by using a modem to dial directly to a workstation; or by using an Internet connection with a Web interface. Remote access may complete a connection via public or private lines.

remote access server — A combination of software and hardware that provides a central access point for multiple users to dial into a network.

Remote Access Service (RAS) — One of the simplest dial-in servers. This software is included with Windows 2000 Server. Note that "RAS" is pronounced *razz*.

Remote Authentication Dial-In User Service (RADIUS) — A server that offers authentication services to the network's access server (which may run the Windows NT or 2000 RAS or Novell's NAS, for example). RADIUS provides a single, centralized point of authentication for dial-in users and is often used by ISPs.

remote computer — The computer that you are controlling or working on via a network connection.

remote control — A remote access method in which the remote user dials into a workstation that is directly attached to a LAN. Software running on both the remote user's computer and the LAN computer allows the remote user to "take over" the LAN workstation.

remote node — A client that has dialed directly into a LAN's remote access server. The LAN treats a remote node like any other client on the LAN, allowing the remote user to perform the same functions he or she could perform while in the office.

remote user — A person working on a computer in a different geographical location from the LAN's server.

repeater — A device used to regenerate a digital signal.

replication — The process of copying Active Directory data to multiple domain controllers. This ensures redundancy so that in case one of the domain controllers fails, clients can still log onto the network, be authenticated, and access resources.

resistance — The opposition to an electric current. Resistance of a wire is a factor of its size and molecular structure.

resolver — Any host on the Internet that needs to look up domain name information.

resource record — The element of a DNS database stored on a name server that contains information about TCP/IP host names and their addresses.

resources — 1) In project management, a term used to refer to staffing, materials, and money. 2) The devices, data, and data storage space provided by a computer, whether standalone or shared.

restore — The process of retrieving files from a backup if the original files are lost or deleted.

Reverse Address Resolution Protocol (RARP) — The reverse of ARP. RARP allows the client to send a broadcast message with the MAC address of a device and receive the device's IP address in reply.

RFI — See *radiofrequency interference*.

ring topology — A network layout in which each node is connected to the two nearest nodes so that the entire network forms a circle. Data are transmitted unidirectionally around the ring. Each workstation accepts and responds to packets addressed to it, then forwards the other packets to the next workstation in the ring.

ring WAN topology — A WAN topology in which each site is connected to two other sites so that the entire WAN forms a ring pattern. This architecture is similar to the LAN ring topology, except that a WAN ring topology connects locations rather than local nodes.

risers — The backbone cabling that provides vertical connections between floors of a building.

RJ-45 — The standard connector used with shielded twisted-pair and unshielded twisted-pair cabling. "RJ" stands for registered jack.

root — A highly privileged user ID that has all rights to create, delete, modify, move, read, write, or execute files on a system. This term may specifically refer to the administrator on a UNIX-based network.

root domain — In Windows 2000 networking, the single domain from which child domains branch out in a domain tree.

root server — A DNS server maintained by ICANN (in North America) that is an authority on how to contact the top-level domains, such as those ending with .com, .edu, .net, .us, and so on. ICANN maintains 13 root servers around the world.

routable — Protocols that can span more than one LAN segment because they carry Network layer and addressing information that can be interpreted by a router.

route — To direct data between networks based on addressing, patterns of usage, and availability of network segments.

router — A multiport device that can connect dissimilar LANs and WANs running at different transmission speeds and using a variety of protocols. In addition, a router can determine the best path for data transmission and perform advanced management functions. Routers operate at the Network layer (Layer 3) or higher of the OSI Model. They are intelligent, protocol-dependent devices.

Routing Information Protocol (RIP) — The oldest routing protocol that is still widely used. RIP does not work in very large network environments where data may have to travel through more than 16 routers to reach their destination (for example, on the Internet). And, compared to other routing protocols, RIP is slower and less secure.

routing protocols — Protocols that assist routers in efficiently managing information flow. For instance, routing protocols determine the best path for data to take between nodes.

routing switch — Another term for a Layer 3 or Layer 4 switch. A routing switch is a hybrid between a router and a switch and can therefore interpret data from Layer 2 and either Layer 3 or Layer 4.

runts — Packet fragments.

runts — Packets that are smaller than a logical topology's minimum packet size. For instance, any Ethernet packet that is smaller than 64 bytes is considered a runt.

sag — See *brownout*.

Samba — An open source software package that provides complete Windows 2000-style file and printer sharing facility.

schema — The description of object types, or classes, and their required and optional attributes that are stored in an NOS's directory.

screening firewall — See *packet-filtering firewall*.

SDH (Synchronous Digital Hierarchy) — The international equivalent of SONET.

security audit — An assessment of an organization's security vulnerabilities. A security audit should be performed at least annually and preferably quarterly or sooner if the network has undergone significant changes. For each risk found, it should rate the severity of a potential breach, as well as its likelihood.

segment — A part of a LAN that is logically separated from other parts of the LAN and that shares a fixed amount of traffic capacity.

segmentation — The process of decreasing the size of data units when moving data from a network segment that can handle larger data units to a network segment that can handle only smaller data units.

self-healing — A characteristic of dual-ring topologies that allows them to automatically reroute traffic along the backup ring if the primary ring becomes severed.

Sequenced Packet Exchange (SPX) — One of the core protocols in the IPX/SPX suite. SPX belongs to the Transport layer of the OSI Model and works in tandem with IPX to ensure that data are received whole, in sequence, and error free.

sequencing — The process of assigning a placeholder to each piece of a data block to allow the receiving node's Transport layer to reassemble the data in the correct order.

serial backbone — The simplest kind of backbone, consisting of two or more hubs connected to each other by a single cable.

Serial Line Internet Protocol (SLIP) — A communications protocol that enables a workstation to connect to a server using a serial connection. SLIP can support only asynchronous communications and IP traffic, and requires some configuration on the client workstation.

server — A computer on the network that manages shared resources. Servers usually have more processing power, memory, and hard disk space than clients. They run network operating software that can manage not only data, but also users, groups, security, and applications on the network.

server clustering — A fault-tolerance technique that links multiple servers together to act as a single server. In this configuration, clustered servers share processing duties and appear as a single server to users. If one server in the cluster fails, the other servers in the cluster will automatically take over its data transaction and storage responsibilities.

server console — The network administrator's primary interface to a NetWare server. Unlike Windows NT, the NetWare server interface is not entirely graphical. NetWare 4.x offers only text-based server menus at the console. NetWare 5.0 allows you to access commands through either a text-based or graphical menu system.

server mirroring — A fault-tolerance technique in which one server duplicates the transactions and data storage of another, identical server. Server mirroring requires a link between the servers and software running on both servers so that the servers can continually synchronize their actions and take over in case the other fails.

server-based network — A network that uses special computers, known as servers, to process data for and facilitate communication between the other computers on the network. See *client/server network*.

server_hello — In the context of SSL encryption, a message issued from the server to the client that confirms the information the server received in the client_hello message and agrees to certain terms of encryption based on the options the client supplied. Depending on the Web server's preferred encryption method, the server may choose to use issue your browser a public key or a digital certificate at this time.

Service Access Point (SAP) — A feature of Ethernet networks that identifies a node or internal process that uses the LLC protocol. Each process between a source and destination node on the network may have a unique SAP.

Service Advertising Protocol (SAP) — A core protocol in the IPX/SPX suite that works in the Application, Presentation, Session, and Transport layers of the OSI Model and runs directly over IPX. NetWare servers and routers use SAP to advertise to the entire network which services they can provide.

service pack — A significant patch to Windows NT or 2000 Server software.

services — The features provided by a network.

session — A connection for data exchange between two parties. The term "session" is most often used in the context of terminal and mainframe communications.

session key — In the context of Kerberos authentication, a key issued to both the client and service by the authentication service that uniquely identifies their session.

Session layer — The fifth layer in the OSI Model. The Session layer establishes and maintains communication between two nodes on the network. It can be considered the "traffic cop" for network communications.

shared Ethernet — A version of Ethernet in which all the nodes share a common channel and a fixed amount of bandwidth.

sheath — The outer cover, or jacket, of a cable.

shell — Another term for command interpreter.

shielded twisted-pair (STP) — A type of cable containing twisted wire pairs that are not only individually insulated, but also surrounded by a shielding made of a metallic substance such as foil. The shielding acts as an antenna, converting the noise into current (assuming that the wire is properly grounded). This current induces an equal, yet opposite current in the twisted pairs it surrounds. The noise on the shielding mirrors the noise on the twisted pairs, and the two cancel each other out.

signal bounce — A phenomenon caused by improper termination on a bus network in which signals travel endlessly between the two ends of the network, preventing new signals from getting through.

signal level — An ANSI standard for T-carrier technology that refers to its Physical layer electrical signaling characteristics. DS0 is the equivalent of one data or voice channel. All other signal levels are multiples of DS0.

signature scanning — The comparison of a file's content with known virus signatures (unique identifying characteristics in the code) in a signature database to determine whether the file is a virus.

simple installation — A NetWare installation option in which the most popular installation options are chosen for you, and the installation takes less time than if you had chosen a custom installation.

Simple Mail Transfer Protocol (SMTP) — A protocol within the TCP/IP suite that is responsible for moving e-mail messages between one mail server and another.

Simple Network Management Protocol (SNMP) — A communication protocol used to manage devices on a TCP/IP network.

simplex — A type of transmission in which signals may travel in only one direction over a medium.

single point of failure — A device or connection on a network that, were it to fail, could cause the entire network to stop functioning.

single-mode fiber — A type of fiber-optic cable with a core of less than 10 microns in diameter that carries light pulses along a single data path from one end of the cable to another. Single-mode fiber can carry data faster and farther than multimode fiber. However, single-mode fiber is more expensive than multimode fiber.

site license — A type of software license that, for a fixed price, allows any number of users in one location to legally access an application.

snap-in — An administrative tool, such as Computer Management, that can be added to the Microsoft Management Console (MMC).

sneakernet — The only means of exchanging data without using a network. Sneakernet requires that data be copied from a computer to a floppy disk, carried (presumably by someone wearing sneakers) to another computer, then copied from the floppy disk onto the second computer.

sniffer — A laptop equipped with a special network adapter and software that performs network analysis. Unlike laptops that may have a network monitoring tool installed, sniffers typically cannot be used for other purposes, because they don't depend on a desktop operating system such as Windows.

Sniffer Portable — Network analyzer software from Network Associates that provides data capture and analysis, node discovery, traffic trending, history, alarm tripping, and utilization prediction.

social engineering — Manipulating relationships to circumvent network security measures and gain access to a system.

socket — A logical address assigned to a specific process running on a computer. A socket forms a virtual connection between the host and client.

soft skills — Skills such as customer relations, leadership ability, and dependability, which are not easily measured, but are nevertheless important in a networking career.

software distribution — The process of automatically transferring a data file or program from the server to a client on the network.

Solaris — Sun Microsystems' proprietary implementation of the UNIX system.

SONET (Synchronous Optical Network) — A WAN technology that provides data transfer rates ranging from 64 Kbps to 39.8 Gbps, using the same time division multiplexing technique used by T-carriers. SONET is the best choice for linking WANs between North America, Europe, and Asia, because it can link directly using the different standards used in different countries.

source code — Computer instructions written in a programming language that is readable by humans. Source code must be translated into a form that is executable by the machine, typically called binary code (for the sequence of zeros and ones) or target code.

source-route bridging — A type of bridging in which the bridge polls the network to determine the best path for data between two points. Source-route bridging is not susceptible to circular routing and, for this reason, is particularly well-suited to WANs.

spanning tree algorithm — A technique used in bridging that can detect circular traffic patterns and modify the way multiple bridges work together in order to avoid such patterns.

spike — A single (or short-lived) jump in a measure of network performance, such as utilization.

sponsors — People in positions of authority who support a project and who can lobby for budget increases necessary to complete the project, appeal to a group of managers to extend a project's deadline, assist with negotiating vendor contracts, and so on.

spread spectrum — A type of radiofrequency transmission in which lower-level signals are distributed over several frequencies simultaneously. Spread spectrum RF is more secure than narrowband RF.

SSL (Secure Sockets Layer) — A method of encrypting TCP/IP transmissions—including Web pages and data entered into Web forms—en route between the client and server using public key encryption technology.

SSL session — In the context of SSL encryption, an association between the client and server that is defined by an agreement on a specific set of encryption techniques. An SSL session allows the client and server to continue to exchange data securely as long as the client is still connected to the server. SSL sessions are established by the SSL handshake protocol.

stackable hub — A type of hub designed to be linked with other hubs in a single telecommunications closet. Stackable hubs linked together logically represent one large hub to the network.

stakeholder — Any person who may be affected by a project, for better or for worse. A stakeholder may be a project participant, user, manager, or vendor.

standalone computer — A computer that uses programs and data only from its local disks and that is not connected to a network.

standalone hub — A type of hub that serves a workgroup of computers that are separate from the rest of the network. A standalone hub may be connected to another hub by a coaxial, fiber-optic, or twisted-pair cable. Such hubs are not typically connected in a hierarchical or daisy-chain fashion.

standards — Documented agreements containing technical specifications or other precise criteria that are used as guidelines to ensure that materials, products, processes, and services suit their intended purpose.

standby UPS — A power supply that provides continuous voltage to a device by switching virtually instantaneously to the battery when it detects a loss of power from the wall outlet. Upon restoration of the power, the standby UPS switches the device to use A/C power again.

star topology — A physical topology in which every node on the network is connected through a central device, such as a hub. Any single physical wire on a star network connects only two devices, so a cabling problem will affect only two nodes. Nodes transmit data to the hub, which then retransmits the data to the rest of the network segment where the destination node can pick it up.

star WAN topology — A WAN topology that mimics the arrangement of star LANs. A single site acts as the central connection point for several other locations.

star-wired bus topology — A hybrid topology in which groups of workstations are connected in a star fashion to hubs that are networked via a single bus.

star-wired ring topology — A hybrid topology that uses the physical layout of a star and the token-passing data transmission method.

static ARP table entry — A record (of an IP address and its associated MAC address) that is manually entered in the ARP table using the ARP utility.

static IP address — An IP address that is manually assigned to a device and remains constant until it is manually changed.

static routing — A technique in which a network administrator programs a router to use specific paths between nodes. Since it does not account for occasional network congestion, failed connections, or device moves, static routing is not optimal.

statistical multiplexing — A method of multiplexing in which each node on a network is assigned a separate time slot for transmission, based on the node's priority and need.

stealth virus — A type of virus that hides itself to prevent detection. Typically, stealth viruses disguise themselves as legitimate programs or replace part of a legitimate program's code with their destructive code.

storage area network (SAN) — A distinct network of multiple storage devices and servers that provides fast, highly available, and highly fault-tolerant access to large quantities of data for a client/server network. SAN uses a proprietary network transmission method (such as Fibre Channel) rather than a traditional network transmission method such as Ethernet.

store and forward mode — A method of switching in which a switch reads the entire data frame into its memory and checks it for accuracy before transmitting it. While this method is more time-consuming than the cut-through method, it allows store and forward switches to transmit data more accurately.

straight-through cable — A twisted-pair patch cable in which the wire terminations in both connectors follow the same scheme.

structured cabling — A method for uniform, enterprise-wide, multivendor cabling systems specified by the TIA/EIA 568 Commercial Building Wiring Standard. Structured cabling is based on a hierarchical design using a high-speed backbone.

subchannel — One of many distinct communication paths established when a channel is multiplexed or modulated.

subnet mask — A special 32-bit number that, when combined with a device's IP address, informs the rest of the network as to what kind of subnet the device is on.

subnets — In an internetwork, the individual networks that are joined together by routers.

subnetting — The process of subdividing a single class of network into multiple, smaller networks.

subprotocols — Small, specialized protocols that work together and belong to a protocol suite.

supported services list — A document (preferably online) that lists every service and software package supported within an organization, plus the names of first- and second-level support contacts for those services or software packages.

surge — A momentary increase in voltage due to distant lightning strikes or electrical problems.

SVC (switched virtual circuit) — Logical, point-to-point connections that rely on switches to determine the optimal path between sender and receiver. ATM technology uses SVCs.

swap file — See *page file*.

switch — 1) A connectivity device that logically subdivides a network into smaller, individual segments. Most switches operate at the Data Link layer of the OSI Model. They interpret MAC address information to determine whether to filter (discard) or forward packets they receive. 2) The letters or words added to a command that allow you to customize a utility's output. Switches are usually preceded by a hyphen or a forward slash character.

switched Ethernet — An Ethernet model that enables multiple nodes to simultaneously transmit and receive data and individually take advantage of more bandwidth because they are assigned separate logical network segments through switching.

switching — A component of a network's logical topology that manages how packets are filtered and forwarded between nodes on the network.

symmetric encryption — A method of encryption that requires the same key to encode the data as is used to decode the cipher text.

symmetric multiprocessing — A method of multiprocessing that splits all operations equally among two or more processors. Windows 2000 Server supports this type of multiprocessing.

symmetrical — A characteristic of transmission technology that provides equal throughput for data traveling both upstream and downstream and is suited to users who both upload and download significant amounts of data.

symmetrical DSL — A variation of DSL that provides equal throughput both upstream and downstream between the customer and the carrier.

synchronous — A transmission method in which data being transmitted and received by nodes must conform to a timing scheme.

System V — The proprietary version of UNIX, originally developed at AT&T Bell Labs, currently distributed by Caldera International and Tarantella, Inc.

T-carriers — The term for any kind of leased line that follows the standards for T1s, fractional T1s, T1Cs, T2s, T3s, or T4s.

T1 — A T-carrier technology that provides 1.544-Mbps throughput and 24 channels for voice, data, video, or audio signals. T1s may use shielded or unshielded twisted-pair, coaxial cable, fiber-optic, or microwave links. Businesses commonly use T1s to connect to their ISP, and phone companies typically use at least one T1 to connect their central offices.

T3 — A T-carrier technology that can carry the equivalent of 672 channels for voice, data, video, or audio, with a maximum data throughput of 44.736 Mbps (typically rounded up to 45 Mbps for purposes of discussion). T3s require either fiber-optic or microwave transmission media.

TCP segment — The portion of a TCP/IP packet that holds TCP data fields and becomes encapsulated by the IP datagram.

TCP/IP core protocols — The subprotocols of the TCP/IP suite.

teleconnector — A transceiver used on LocalTalk networks. The teleconnector is linked to the node's serial port on one side, and to the wall jack on the other side.

Telnet — A terminal emulation protocol used to log on to remote hosts using the TCP/IP protocol. Telnet resides in the Application layer of the TCP/IP suite.

terminal — A device with little (if any) of its own processing or disk capacity that depends on a host to supply it with applications and data-processing services.

Terminal Access Controller Access Control System (TACACS) — A centralized authentication system for remote access servers that is similar to RADIUS.

terminal adapter (TA) — Devices used to convert digital signals into analog signals for use with ISDN phones and other analog devices. Terminal adapters are sometimes called ISDN modems.

terminal equipment (TE) — Devices that connect computers to the ISDN line. Terminal equipment may include standalone devices or cards (similar to the network adapters used on Ethernet and Token Ring networks) or ISDN routers.

Thicknet — A type of coaxial cable, also known as thickwire Ethernet, that is a rigid cable approximately 1-cm thick. Thicknet was used for the original Ethernet networks. Because it is often covered with a yellow sheath, Thicknet is also called "yellow Ethernet." IEEE has designated Thicknet as 10Base5 Ethernet, with the "10" representing its throughput of 10 Mbps, the "Base" standing for baseband transmission, and the "5" representing the maximum segment length of a Thicknet cable, 500 m.

thickwire Ethernet — See *Thicknet*.

thin client — A type of software that enables a client to accomplish functions over a network while utilizing little of the client workstation's resources and, instead, relying on the server to carry the processing burden.

thin Ethernet — See *Thinnet*.

Thinnet — A type of coaxial cable, also known as thin Ethernet, that was the most popular medium for Ethernet LANs in the 1980s. Like Thicknet, Thinnet is rarely used on modern networks. IEEE has designated Thinnet as 10Base2 Ethernet, with the "10" representing its data transmission rate of 10 Mbps, the "Base" representing the fact that it uses baseband transmission, and the "2" roughly representing its maximum segment length of 185 m.

thread — A well-defined, self-contained subset of a process. Using threads within a process enables a program to efficiently perform related, multiple, simultaneous activities. Threads are also used to enable processes to use multiple processors on SMP systems.

throughput — The amount of data that a medium can transmit during a given period of time. Throughput is usually measured in megabits (1,000,000 bits) per second, or Mbps. The physical nature of every transmission medium determines its potential throughput.

ticket — In Kerberos terminology, a temporary set of credentials that a client uses to prove that its identity has been validated by the authentication service.

ticket granting service (TGS) — In Kerberos terminology, an application that runs on the key distribution center that issues ticket granting tickets to clients so that they need not request a new ticket for each new service they want to access.

ticket granting ticket (TGT) — In Kerberos terminology, a ticket that enables a user to be accepted as a validated principal by multiple services.

tiered WAN topology — A WAN topology in which sites are connected in star or ring formations and interconnected at different levels with the interconnection points organized into layers.

time division multiplexing (TDM) — A method of multiplexing that assigns a time slot in the flow of communications to every node on the network and in that time slot, carries data from that node.

time domain reflector (TDR) — A high-end instrument for testing the qualities of a cable. It works by issuing a signal on a cable and measuring the way in which the signal bounces back (or reflects) to the TDR.

time-dependent virus — A virus programmed to activate on a particular date. This type of virus, also known as a "time bomb," can remain dormant and harmless until its activation date arrives.

time-sharing system — A computing system to which users must attach directly so as to use the shared resources of the computer.

TLS (Transport Layer Security) — A version of SSL being standardized by the Internet Engineering Task Force (IETF). With TLS, IETF aims to create a version of SSL that will encrypt UDP as well as TCP transmissions. TLS, which will likely be supported by new Web browsers, uses slightly different encryption algorithms than SSL, but otherwise is very similar to the most recent version of SSL.

token — A special control frame that indicates to the rest of the network that a particular node has the right to transmit data.

token passing — A means of data transmission in which a 3-byte packet, called a token, is passed around the network in a round-robin fashion.

Token Ring — A networking technology developed by IBM in the 1980s. It relies upon direct links between nodes and a ring topology, using tokens to allow nodes to transmit data.

Token Ring media filter — A device that enables a DB-9 cable and a type 1 IBM cable to be connected.

tone generator — A small electronic device that issues a signal on a wire pair. When used in conjunction with a tone locator, it can help locate the termination of a wire pair.

tone locator—A small electronic device that emits a tone when it detects electrical activity on a wire pair. When used in conjunction with a tone generator, it can help locate the termination of a wire pair.

top-level domain (TLD) — The highest-level category used to distinguish domain names—for example, .org, .com, .net. A TLD is also known as the domain suffix.

topology — The physical layout of a computer network.

traceroute (or tracert) — A TCP/IP troubleshooting utility that uses ICMP to trace the path from one networked node to another, identifying all intermediate hops between the two nodes. Traceroute is useful for determining router or subnet connectivity problems.

traffic — The data transmission and processing activity taking place on a computer network at any given time.

traffic monitoring — Determining how much processing activity is taking place on a network or network segment and notifying administrators when a segment becomes overloaded.

transceiver (transmitter/receiver) — A device that both transmits and receives signals. Since a transceiver is concerned with applying signals to the wire, it belongs in the Physical layer of the OSI Model. Many different types of transceivers exist in networking.

translational bridging — A type of bridging in which bridges can not only forward packets, but also translate packets between one logical topology and another. For instance, translational bridging can connect Token Ring and Ethernet networks.

transmission — In networking, the application of data signals to a medium or the progress of data signals over a medium from one point to another.

Transmission Control Protocol (TCP) — A core protocol of the TCP/IP suite. TCP belongs to the Transport layer and provides reliable data delivery services.

transmission media — The means through which data are transmitted and received. Transmission media may be physical, such as wire or cable, or atmospheric (wireless), such as radio waves.

transparent bridging — The method of bridging used on most Ethernet networks.

Transport layer — The fourth layer of the OSI Model. The Transport layer is primarily responsible for ensuring that data are transferred from point A to point B (which may or may not be on the same network segment) reliably and without errors.

tree — A logical representation of multiple, hierarchical levels in a directory. It is called a tree because the whole structure shares a common starting point (the root) and from that point extends branches (or containers), which may extend additional branches, and so on.

Trivial File Transfer Protocol (TFTP) — A TCP/IP Application layer protocol that enables file transfers between computers. Unlike FTP, TFTP relies on UDP at the Transport layer and does not require a user to log onto the remote host.

Trojan horse — A program that disguises itself as something useful but actually harms your system.

trust relationship — The relationship between two domains on a Windows 2000 or Windows NT network that allows a domain controller from one domain to authenticate users from the other domain.

tunneling — The process of encapsulating one protocol to make it appear as another type of protocol.

twist ratio — The number of twists per meter or foot in a twisted-pair cable.

twisted-pair (TP) — A type of cable similar to telephone wiring that consists of color-coded pairs of insulated copper wires, each with a diameter of 0.4 to 0.8 mm, twisted around each other and encased in plastic coating.

two-way transitive trust — The security relationship between domains in the same domain tree in which one domain grants every other domain in the tree access to its resources and, in turn, that domain can access other domains' resources. When a new domain is added to a tree, it immediately shares a two-way trust with the other domains in the tree.

type 1 IBM connector — A type of Token Ring connector that uses interlocking tabs that snap into an identical connector when one is flipped upside-down, making for a secure connection. Type 1 IBM connectors are used on STP-based Token Ring networks.

typeful — A way of denoting an object's context in which the Organization and Organizational Unit designators ("O" and "OU," respectively) are included. For example, OU=Inv.OU=Ops.OU=Corp.O=Sutkin.

typeless — A way of denoting an object's context in which the Organization and Organizational Unit designators ("O" and "OU," respectively) are omitted. For example, Inv.Ops.Corp.Sutkin.

unicast address — A type of IPv6 address that represents a single interface on a device. An IPv6 unicast address begins with either FFC0 or FF80.

Uniform Resource Locator (URL) — A standard means of identifying every Web page, which specifies the service used, its server's host name, and its HTML page or script name.

uninterruptible power supply (UPS) — A battery-operated power source directly attached to one or more devices and to a power supply (such as a wall outlet), which prevents undesired features of the power source from harming the device or interrupting its services.

Universal Disk Format (UDF) — A file system used on CD-ROMs and digital video disc (DVD) media.

universal group — A group on a Windows 2000 network that allows members from one domain to access resources in multiple domains and forests.

unqualified host name — A TCP/IP host name minus its prefix and suffix.

unshielded twisted-pair (UTP) — A type of cabling that consists of one or more insulated wire pairs encased in a plastic sheath. As its name implies, UTP does not contain additional shielding for the twisted pairs. As a result, UTP is both less expensive and less resistant to noise than STP.

upgrade — A major change to the existing code in a software program, which may or may not be offered free from a vendor and may or may not be comprehensive enough to substitute for the original program.

upstream — A term used to describe data traffic that flows from a customer's site to the local carrier's POP. In symmetrical communications, upstream throughput is usually much lower than downstream throughput. In symmetrical communications, upstream and downstream throughputs are equal.

USB (universal serial bus) port — A standard external bus that can be used to connect multiple types of peripherals, including modems, mice, and network adapters, to a computer. The original USB standard was capable of transmitting only 12 Mbps of data; a new standard is capable of transmitting 480 Mbps of data.

user — A person who uses a computer.

User Datagram Protocol (UDP) — A core protocol in the TCP/IP suite that sits in the Transport layer, between the Internet layer and the Application layer of the TCP/IP model. UDP is a connectionless transport service.

user principal name (UPN) — The preferred Active Directory naming convention for objects when used in informal situations. This name looks like a familiar Internet address, including the positioning of the domain name after the @ sign. UPNs are typically used for e-mail and related Internet services.

user principal name (UPN) suffix — The portion of a universal principal name (in Windows 2000 Active Directory's naming conventions) that follows the @ sign.

vampire tap — A connector used on Thicknet MAUs that pierces a hole in the coaxial cable, thus completing a connection between the metal tooth in the vampire tap and the copper core of the cable.

vault — A large tape storage library.

virtual circuits — Connections between network nodes that, while based on potentially disparate physical links, logically appear to be direct, dedicated links between those nodes.

virtual local area network (VLAN) — A network within a network that is logically defined by grouping its devices' switch ports in the same broadcast domain. A VLAN can consist of servers, workstations, printers, routers, or any other network device you can connect to a switch.

virtual memory — Memory that is logically carved out of space on the hard disk and added to physical memory (RAM).

virtual private network (VPN) — A logically constructed WAN that uses existing public transmission systems. VPNs can be created through the use of software or combined software and hardware solutions. This type of network allows an organization to carve out a private WAN on the Internet (or, less commonly over leased lines) that serves only its offices, while keeping the data secure and isolated from other (public) traffic.

virus — A program that replicates itself so as to infect more computers, either through network connections or through floppy disks passed among users. Viruses may damage files or systems or simply annoy users by flashing messages or pictures on the screen or by causing the keyboard to beep.

virus hoax — A rumor, or false alert, about a dangerous, new virus that could supposedly cause serious damage to your workstation.

Voice over IP (VoIP) — The provision of telephone service over a TCP/IP network. (Pronounced "voyp".) One form of VoIP is Internet telephony.

volt — Measurement used to describe the degree of pressure an electrical current exerts on a conductor.

volt-amp (VA) — A measure of electrical power. A volt-amp is the product of the voltage and current (measured in amps) of the electricity on a line.

voltage — The pressure (sometimes informally referred to as the strength) of an electrical current.

voltmeter — Device used to measure voltage (or electrical pressure) on an electrical circuit.

WAN — See *wide area network*.

WAN link — The line that connects one location on a WAN with another location.

WAN topology — The physical layout, or pattern, of locations on a wide area network (WAN).

wavelength — The distance between corresponding points on a wave's cycle. Wavelength is inversely proportional to frequency.

wavelength division multiplexing (WDM) — A multiplexing technique in which each signal on a fiber-optic cable is assigned a different wavelength, which equates to its own subchannel. Each wavelength is modulated with a data signal. In this manner multiple signals can be simultaneously transmitted in the same direction over a length of fiber.

Webcasting — A broadcast transmission from one Internet-attached node to multiple other Internet-attached nodes.

well-known ports — TCP/IP port numbers 0 to 1023, so called because they were long ago assigned by Internet authorities to popular services (for example, FTP and Telnet), and are therefore well known and frequently used.

wide area network (WAN) — A network connecting geographically distinct locations, which may or may not belong to the same organization. The Internet is an example of a very large WAN.

Windows Internet Naming Service (WINS) — A service that resolves NetBIOS names with IP addresses. WINS is used exclusively with systems that use NetBIOS—therefore, it is usually found on Windows-based systems.

winipcfg — The TCP/IP configuration and management utility for use with Windows 9x systems. Winipcfg differs from ipconfig in that it supplies a graphical user interface.

wireless — Networks that transmit signals through the atmosphere via infrared or RF signaling.

wizard — A simple graphical program that assists the user in performing complex tasks, such as configuring a NIC on a server.

workgroup — A group of interconnected computers that share each others' resources without relying on a central file server.

workstation — A computer that typically runs a desktop operating system and connects to a network.

World Wide Web (WWW or Web) — A collection of internetworked servers that share resources and exchange information according to specific protocols and formats.

worm — An unwanted program that travels between computers and across networks. Although worms do not alter other programs as viruses do, they may carry viruses.

X.25 — An analog packet switched WAN technology optimized for long-distance data transmission and standardized by the ITU in the mid-1970s. X.25 can support 2-Mbps throughput. It was originally developed and used for communications between mainframe computers and remote terminals.

xDSL — Term used to refer to all varieties of DSL.

zone — The group of machines managed by a DNS server.